Oracle® Communications Security Shield Cloud Service

User's Guide

F24354-20
February 2024

Oracle Communications Security Shield Cloud Service User's Guide,

F24354-20

Contents

4 Phone Number Formatting

5 Common Controls and Actions

6 The Dashboard

7 Access Control Lists

8 Outbound Number Management

9 Number Lookup

10 Activity Logs

11 Notifications

12 Settings

13 Security Shield Call Traffic Analytics

About This Guide

The Security Shield User's Guide explains how to manage security for the call traffic traversing your Oracle Session Border Controller with the Oracle® Communications Security Shield Cloud Service (Security Shield). This guide provides network diagrams and instructions for setting the controls and actions that you can apply to the call traffic, as well as information about activity logs.

Security Shield Operations Documented in this Guide

- Viewing and working with the Dashboard
- Creating and managing access control lists
- Viewing and working with activity logs
- Configuring General Threat Protection, Threat Vector Thresholds, Domain Thresholds, Call Type Classifications, and Reputation Score Classifications
- Viewing analytics data

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.

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.

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
June 2021	21.0.0.0.0
August 2021	21.1.0.0.0
November 2021	21.2.0.0.0
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
January 2024	23.3.1.0.0 • Adds the Trusted Enterprise Calls subscription
February 2024	24.0.0.0.0

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
Security Shield Overview

Oracle® Communications Security Shield Cloud Service (Security Shield) is a cloud service that restores trust in the phone channel.

Security Shield assesses risk and verifies the caller ID to protect against fraud and scams. The primary services that Security Shield provides are fraud and spam mitigation and trusted enterprise calls.

Security Shield provides rich analytics that you can use to assess the deep call insights provided to examine the call center key performance indicators as well as fraud and spam details to facilitate investigations.

Topics:

Fraud and Spam Mitigation Overview

Oracle® Communications Security Shield Cloud Service (Security Shield) identifies suspicious use of phone numbers and detects anomalies in calling patterns to flag or block fraudulent, scam, and spam calls.

Security Shield dynamically assess the risk for each call by using traffic behavior data, deterministic data, and intelligence data using machine learning. Deterministic data includes data attributes about a phone number such as line type and telecom carrier of record, whether the number is allocated or not, and many others. Intelligence data includes crowd-sourced information about fraudulent calls. Security Shield uses machine learning techniques to detect anomalies and identify potential fraud based on traffic behavior. Security Shield uses all these data inputs to classify the risk probability as well as threat prediction.

Trusted Enterprise Calls

The Oracle® Communications Security Shield Cloud Service (Security Shield) Trusted Enterprise Calls service enables you to verify your outbound calls using STIR/SHAKEN call authentication to reduce call spoofing and fraud. Security Shield can automate the end-to-end process of digitally signing calls using STIR/SHAKEN for you.

The Trusted Enterprise Calls service ensures that calls from trusted sources are more likely to be answered by your customers, which helps with retention, revenue targets, and customer satisfaction. You can purchase either a bundled service that includes the STIR/SHAKEN call authentication or you can bring your own license from an approved STIR/SHAKEN call authentication service.

> **Note:**
>
> Currently, Security Shield supports only Transunion TruContact Caller ID Authentication (formerly known as Neustar Enterprise Certified Caller).

See SPL Requirements for Trusted Enterprise Calls.

SPL Requirements for Trusted Enterprise Calls

The 24.0.0.0.0 release adds new SPL options to send only inbound or outbound calls to the Security Shield cloud. You must use SPL 1.1.4 or higher for the Trusted Enterprise Calls subscription.

> **Important:**
>
> 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.

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
```

General Features

Oracle® Communications Security Shield Cloud Service (Security Shield) provides the following features.

- A Dashboard with graphical visualizations of your phone traffic. The Dashboard shows which events were detected, the enforcement actions applied, and more. The Dashboard also provides service management
- Call admission based on customer-managed “allow” lists and "blocklists".

Security Shield Deplyoment Model

Oracle® Communications Security Shield Cloud Service (Security Shield integrates with your Oracle Communications Session Border Controller or with your Oracle Communications Session Router. The deployment includes the Cloud Communication Service (CCS).

The Oracle Cloud Infrastructure hosts Security Shield along with other components that Security Shield uses for operations such as the Dashboard, analytics, third party integration, the data store, and other services.

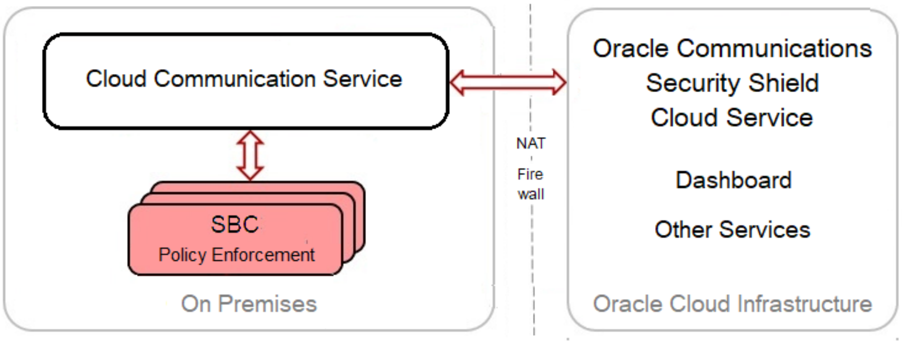
Security Shield Components

The following information explains the components in an Oracle® Communications Security Shield Cloud Service (Security Shield) deployment.

A Security Shield deployment includes the Oracle Communications Session Border Controller (SBC) and the Cloud Communication Service (CCS). The Oracle Cloud Infrastructure hosts Security Shield along with other components that Security Shield uses for operations such as the Dashboard, analytics, phone intelligence look-ups, the data store, and other services. The Cloud Communications Service (CCS) and the SBC reside on-premises.

Diagram of Security Shield Components

The following diagram shows the components in a Security Shield deployment.


Cloud Communication Service
SBC
Policy Enforcement
On Premises
NAT
Fire wall
Oracle Communications Security Shield Cloud Service
Dashboard
Other Services
Oracle Cloud Infrastructure

Session Border Controller

The SBC serves as the entry point for calls and acts as the enforcement point for implementing the actions that Security Shield instructs. The SBC also reports the end of a call, the reason for termination, and call timers, which Security Shield uses for reputation assessment and threat detection.

Cloud Communication Service

The CCS establishes a secure ground-to-cloud tunnel for on-premises Security Shield components to communicate with Security Shield components in the Oracle Cloud Infrastructure.

Oracle Communications Security Shield Cloud Service

Security Shield hosts the Web GUI, which displays tabs where you can configure, manage, and maintain the service.

Security Shield applies rules, provides call behavior analytics, sends the enforcement actions to the session border controller. Security Shield combines various sources of information to instruct the session border controller about which actions to perform on a call. Security Shield works predominantly pre-answer, but also supports post-answer control. The enforcement actions, which you can specify, can include actions such as allowing, blocking, and redirecting the call to a different destination.

Security Shield also integrates with the Data Analytics Cloud Service, which is a combination of multiple services designed to perform advanced analytics. The Data Analytics Cloud Service stores SIP INVITE messages and policy results in a data lake for analytics.

Session Border Controller and Session Router

Either the Session Border Controller (SBC) or the Session Router (SR) serves as the entry point for calls and acts as the enforcement point for implementing the actions that Oracle® Communications Security Shield Cloud ServiceSecurity Shield) instructs.

The SBC or SR also reports the end of a call, the reason for termination, and call timers, which Security Shield uses for reputation assessment and threat detection. The SBC and SR integrate with Security Shield through a proprietary REST API over Transport Layer Security.

Cloud Communication Service

The Cloud Communication Service (CCS) establishes a secure ground-to-cloud tunnel for on-premises Oracle® Communications Security Shield Cloud Service (Security Shield) components to communicate with Security Shield components in the Oracle Cloud Infrastructure.

Oracle® Communications Security Shield Cloud Service

Oracle® Communications Security Shield Cloud Service refers to the actual Security Shield service. Security Shield evaluates SIP-based calls sent from the Session Border Controller (SBC) or Session Router (SR) to Security Shield. Security Shield sends instructions back to the SBC or SR for each call it processes for how to handle the call along with any information to add to the call signaling.

Security Shield provides the following functions and services:

- Number normalization
- Non-conformant number handling

- Access control Lists
- Integration with third-party service and data providers
- Fraud and spam mitigation service
- Trusted Enterprise Call service
- A Dashboard where you can view information about call traffic, service metrics, and information, as well as manage the service
- Security Shield can also provide advanced analytics
- Additional call signaling information

Security Shield Subscriptions

You can purchase Oracle® Communications Security Shield Cloud Service (Security Shield) by way of the following base (stand-alone) and add-on subscriptions.

For more details about the features available in each subscription, see Security Shield Features per Subscription.

Subscription	Use Case	Type	Description
Oracle Communications Security Shield Cloud Service	Fraud and spam mitigation	Base	Helps protect telephony networks from malicious actors that launch network attacks such as Telephony Denial of Service (TDoS).
Oracle Communications Security Shield Cloud Service, Premium Edition	Fraud and spam mitigation	Base	Helps protect telephony networks from malicious actors that launch network attacks using machine-learning and third-party data. Provides enhanced dynamic risk assessment and call insights. Provides access to advanced analytics capabilities.
Oracle Communications Security Shield Cloud Service, Trusted Enterprise Calls	Trusted Enterprise Calls	Base	Bolsters call answering rates for outbound calls and mitigates enterprise spoofing. For digitally signing calls using STIR/SHAKEN authentication, you must either purchase the two add-on subscriptions for Trusted Enterprise Calls or bring your own license from a supported STIR/SHAKEN call authentication service.

Subscription	Use Case	Type	Description
Oracle Communications Security Shield Cloud Service, Trusted Enterprise Calls, Attested Call	Trusted Enterprise Calls	Add-on	An optional, add-on service to the Oracle Communications Security Shield Cloud Service, Trusted Enterprise Calls subscription. Bundles the digital signing of calls using STIR/SHAKEN authentication with the Oracle Communications Security Shield, Trusted Enterprise Calls subscription.
Oracle Communications Security Shield Cloud Service, Trusted Enterprise Calls, Attested Number	Trusted Enterprise Calls	Add-on	An optional, add-on service to the Oracle Communications Security Shield Cloud Service, Trusted Enterprise Calls. Bundles the certification and verification of the legitimate user of the CallerID for use in STIR/SHAKEN authentication with the Oracle Communications Security Shield, Trusted Enterprise Calls subscription.

Contact Oracle Sales for more information about the subscriptions.

Security Shield Features per Subscription

The following table lists the Oracle® Communications Security Shield Cloud Service (Security Shield) subscriptions and the features available with each type

Table 1-1 Oracle Communications Security Shield Cloud Service Subscriptions

Features	Standard	Premium Edition	Trusted Enterprise Calls	Trusted Enterprise Calls - Attested Call	Trusted Enterprise Calls - Attested Number
Calling Number Normalization	√	√	√		
Access Control List	√	√	√		

Table 1-1 (Cont.) Oracle Communications Security Shield Cloud Service Subscriptions

Features	Standard	Premium Edition	Trusted Enterprise Calls	Trusted Enterprise Calls - Attested Call	Trusted Enterprise Calls - Attested Number
Dashboard with Service Information	√	√	√		
Spoofing Detection	Basic	Advanced			
Traffic Pumping Detection	√	√			
Toll Fraud	√	√			
Routing Policy Enforced	√	√	√		
Dynamic Risk Assessment Using Machine Learning		√			
Indication of Fraud and Spam Risk		√			
Call Tag (customer header) for Inbound Calls		√			
Advanced Analytics		√	√		
Spam Tag Mitigation of Outbound Calls			√		
Digitally Signing Calls Using STIR/ SHAKEN Call Authentication			By way of a third-party service or bundled with add-on subscriptions	√ (For the bundled service)	√ (For the bundled service)

2

Fraud and Spam Detection

The following information explains how Oracle® Communications Security Shield Cloud Service (Security Shield) features and operations work to detect fraud and spam in your telephony network.

Topics:

Why Risk Assessment and Detecting Fraud and SPAM Calls is Challenging

Fraudulent calls (including robocalls, reconnaissance, and others) look like every other phone call when they arrive at your Call Center or (Unified) Voice Communications Platform. Detecting fraud is often challenging due to several factors.

Examples of fraud are often rare relative to the broader base of normal transactions. The imbalance in the data makes using classification algorithms difficult because there is not enough “signal” in the data to produce an accurate model.

Patterns of fraud change quickly. Using historical data, even when you have enough examples, may not be helpful as fraudsters constantly change tactics. A model that learned patterns of past fraud well may still not be able to detect future instances of fraud. More importantly, the ability to rebuild models on the latest data and redeploy those models within hours, not days, weeks, or months, enables detecting new patterns of fraud while the patterns are still relevant.

The Benefits of Dynamic Risk Assessment

Detection of anomalous behavior and classification are problems typically solved using Machine Learning.

While the rules may work great initially, they become less useful over time as technology evolves and attack methods change. Bad actors want to achieve their goals with as little effort as possible, so they will not waste resources trying the same approach that does not work again and again. Bad actors will find a way around the static barrier. We do not want predictive algorithms to memorize input data. Rather, we want the algorithms to generalize to more effectively handle data they have not encountered before. Assigning a probability to potential fraud can help prioritize which cases to investigate first. We say “potential” fraud because machine learning models are not perfect, they can make mistakes.

Dynamic Risk Assessment Using Machine Learning with the Premium Edition

Oracle® Communications Security Shield Cloud Service (Security Shield) uses common machine learning techniques for identifying potential fraud including Anomaly Detection, Classification, and Clustering.

Security Shield uses unsupervised machine learning for outlier detection and segmentation of abnormal and risky behaviors from normal behaviors. Security Shield clusters the data first to get a “first order” grouping of similar cases. Then Security Shield can build an anomaly detection model on the records assigned to each cluster, which allows finding unusual cases within each cluster.

Using supervised machine learning, based on network data (number attributes) and listings (customer feedback and traffic pattern detection outputs) Security Shield can classify risky transactions, risky prefixes, and risky carriers. Higher risk scores indicate a higher likelihood of fraud, enabling organizations to prioritize their resources and focus on specific calls or users that warrant further investigation.

The preceding techniques, by themselves, may produce useful results but could result in too many false positives. To help mitigate the problem, Security Shield combines multiple machine learning techniques and models to improve the accuracy and robustness of fraud detection. Applying the notion that multiple sources are better than one source, Security Shield uses one or more each of anomaly detection, classification, or clustering models as input for an ensemble of techniques used to identify which calls are potentially fraudulent. If any model identifies potential fraud, the call is internally classified as such. Security Shield limits the potential fraud cases to those where multiple approaches agree on potential fraud.

Given the imperfect performance of machine learning algorithms, a call flagged as fraud may only merit further investigation. By assigning a risk score and risk category, Security Shield indicates the probability of potential fraud. Security Shield determines the risk probability on a scale of 0 to 100 points.

The score, threat data, and number-related data can help prioritize which cases to investigate first and how to treat potential fraudulent calls.

Security Shield Risk Assessment Data Inputs

Oracle® Communications Security Shield Cloud Service (Security Shield) uses phone numbers to monitor traffic patterns, determine phone number-related attributes, and intelligence data.

- Traffic Patterns: Activity from a phone number and the range it belongs to, call duration, and diversity of called numbers.
- Phone Number Attributes: The carrier of record, line type, number type, tenure (how long is number seen), diversity of called numbers.
- Intelligence Data: Third party fraud database, customer feedback (labeled data, other).

The model is dynamic and adaptive and takes in many inputs and variables into account to determine risk including:

Risk and Fraud Investigation Recommendations

While the Oracle® Communications Security Shield Cloud Service (Security Shield) risk classifications and threat classifications provide useful information for determining the call treatment, the flagged calls (by risk classification or threat classification) may warrant only further investigation.

When you investigate a possible risk or fraud call or determine which call actions to apply, consider the following recommendations.

- Understand why a call is identified as fraud, which may be critical to opening an investigation. Security Shield provides call insights to help you understand why a call is flagged as potential fraud or high risk.
- Use the analytics capability to find the additional details, such as call insights, and examine the traffic pattern.
- Determine if the caller is an existing customer, which type of customer (residential or business), or use any other information that can be a proxy to determine if it is a good caller or not (such as annotation in CRM).

User Feedback

Oracle appreciates your feedback on how Oracle® Communications Security Shield Cloud Service (Security Shield) assessed the risk of a call. Customer feedback, for example by labeled data, is how supervised machine-learning techniques learn.

Your feedback improves the detection of potential fraud and new tactics of fraud. Your feedback will also help Oracle to improve higher accuracy of the fraud and risk prediction for you.

Given the imperfect performance of machine learning algorithms, Security Shield involving millions of real-time calls daily, some degree of error is expected. Your feedback, in combination with our own internal monitoring and investigation is important to reduce the false positive and false negative rate.

Too many false positives, where calls are identified as potential fraud when they are not fraudulent, can have significant negative side effects. If each instance of suspected fraud needs to be manually investigated, such investigation is expensive and time consuming, potentially allowing other real instances of fraud to go unchecked.

Dynamic Risk Assessment Using Machine Learning with the Standard Service

Oracle® Communications Security Shield Cloud Service (Security Shield) – Standard Service verifies the calling phone number, tracks behavior, and determines the risk score. The risk score expresses a probability of risk. You can configure call treatment for calls based on the phone number, behavior, or risk.

Security Shield determines the risk probability on a scale of 0 to 100 points.

Call Flooding Mitigation

Artificially high call attempt rates, called “call flooding”, can severely impact your business by overloading your phone lines. Call flooding, whether intentional or unintentional, can slow or prevent legitimate calls from getting through and possibly create a service outage.

Intentional call flooding includes calls from attackers who want to harm or harass the target entity. Unintentional call flooding might result from a call to action on social media or an error in the configuration of call traffic. Oracle® Communications Security Shield Cloud Service (Security Shield) can detect and mitigate call flooding by way of parameters you set in the Threat Vector Thresholds configuration. You can view data about call flooding activity in your network on the Security Shield Dashboard.

> **Note:**
>
> Security Shield does not count multiple calls in a call flooding scenario against your subscription total. It counts too-frequent multiple calls to a single number as one call, regardless of the enforcement action.

Threat Vector Thresholds

Edit Threat Vector Thresholds

Security Shield Enforcement Actions

You can configure Oracle® Communications Security Shield Cloud Service (Security Shield) to apply a call treatment other than ALLOW.

The following list describes the enforcement actions that (Security Shield) can perform.

Allow (default)

Trigger and Description—You configure ALLOW in an Access Control List, Non-E164 Number, Anonymous Caller, Call Type, and Calls Classification. Another condition for ALLOW is when Security Shield processing takes long and a time out occurs.

Required Data—NA

Inbound or Outbound—Both

Enforcement Location—NA

Block per Access Control Lists

Trigger and Description—When Security Shield determines that the caller exists on a Access Control List with the action set to Block, it blocks the call. Because Security Shield enforces the blocking action prior to call establishment, no call information traverses the enforcement point into the network. Security Shield also uses random response codes (from a list of valid codes) to obfuscate the actual reason for blocking a call.

Required Data—User-defined deny list

Inbound or Outbound—Both

Enforcement Point—Session Border Controller or Session Router

Block Due to Risk Score Action or Threat (call type) Action

Trigger and Description—For a given risk category or call type for which the enforcement action is set to BLOCK, Security Shield blocks the call when the call falls into that risk category or call type. Security Shield also uses random response codes (from a list of valid codes) to obfuscate the actual reason for blocking a call.

Required Data—Risk Category or Call Type

Inbound or Outbound—Both

Enforcement Location—Session Border Controller or Session Router

Exclude per Access Control Lists

Trigger and Description—When you configure Exclude for a phone number on an access control list, Security Shield allows inbound calls while still evaluating against TDoS, Traffic Pumping, Spoofing, and Toll Fraud threat detection. Exclude ignores the risk assessment and classifies excluded calls as "Good". The Exclude action does not evaluate against Fraud Risk, Spam Risk, and Call Center call detection.

Required Data—Access Control List

Inbound or Outbound—Inbound

Enforcement Location—NA

Rate Limiting Due to Traffic Pumping

Trigger and Description—Rate limiting applies only to Traffic Pumping. When the attempted call rate reaches the threshold you configured for Traffic Pumping, Security Shield randomly drops calls based on the configured rate limit.Security Shield drops calls silently to the rate of calls defined by the configured rate limit. You set the call attempt rate threshold on the Threat Vector Thresholds tab on the Autonomous Threat Protection page. You can set a threshold from 1-10,000.

Required Data—NA

Inbound or Outbound—Inbound

Enforcement Location—NA

Re-Direct Due to Risk Score Action or Threat (call type) Action

Trigger and Description—For a given risk category or call type for which the enforcement action is set to REDIRECT, Security Shield redirects the call to the configured new target number. When rerouting the call, Security Shield provides the relevant call routing information for the enforcement points to route the call.

An example of rerouting a call is when you want skilled agents or your security team handle the caller validation. Another example is a call routed to an Interactive Voice Response system with minimal permission instead of a live agent.

Redirect Due to Access Control List

Trigger and Description—When Security Shield determines that the caller exists on a Access Control List with the action set to REDIRECT, it reroutes the call to new destination.

For example, you can reroute known fraud numbers or internal numbers that need no further authentication or validation by way of an Access Control List.

Mid-Call Updates

To avoid lengthy post-dial delays, Oracle® Communications Security Shield Cloud Service (Security Shield) uses a guard timer to respond back within a maximum time interval. When this happens, SSecurity Shield sends back an enforcement action along with other available information. The default action is ALLOW, but in some circumstances the action may be of one of the other types.

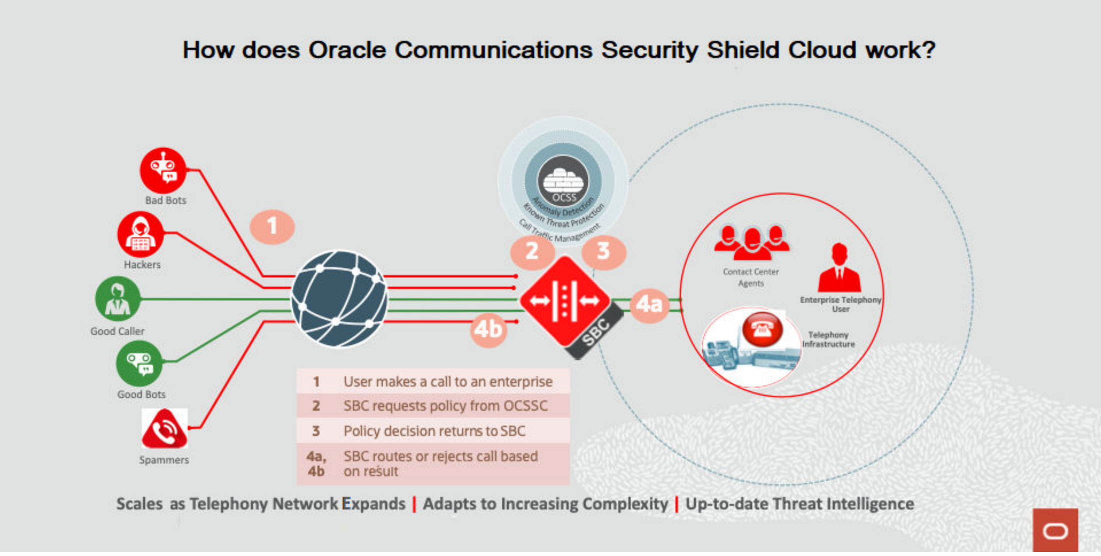
When Security Shield compiles a full response after the guard timer expires, and the initial enforcement action was ALLOW, Security Shield updates the enforcement action (based on the risk category or call type) and sends the updated action back. When calls are BLOCKED or REDIRECTED based on a partial response, Security Shield sends no mid-call update back. If the call still exists on the Oracle Communications Session Border Controller, it is terminated.

> **Note:**
>
> If you change the Cloud Communication Service (CCS) public IP address (WAN interface), it may take up to twenty four hours for mid-call updates to resume.

See Scenarios for Enabling or Disabling Mid-Call Updates

Call Flow with Security Shield in the Network

Either the Oracle Communications Session Border Controller (SBC) or the Oracle Session Router (OR) sends a REST API request to Oracle® Communications Security Shield Cloud Service (Security Shield) for each new call configured for Security Shield. In the API calls, the SBC sends specific data from the INVITE and BYE to Security Shield. Security Shield communicates the enforcement action to the SBC, which applies the action to the call.



How does Oracle Communications Security Shield Cloud work?

1	User makes a call to an enterprise
2	SBC requests policy from OCSSC
3	Policy decision returns to SBC
4a, 4b	SBC routes or rejects call based on resúlt

Scales as Telephony Network Expands | Adapts to Increasing Complexity | Up-to-date Threat Intelligence

SBC to Security Shield Connectivity

The Oracle Communications Session Border Controller (SBC) or the Oracle Communications Session Router (SR) uses the following process when connecting to Oracle® Communications Security Shield Cloud Service (Security Shield):

- The SBC waits up to two seconds for a policy response from Security Shield. After the time out period, the SBC allows the call automatically.
- When five consecutive request timeouts occur in a ten second window, the SBC stops sending requests to Security Shield for fifteen seconds. During this time period, the SBC automatically allows all calls.
- After the initial fifteen second delay, the SBC samples traffic by sending every sixth message to Security Shield and waiting ten seconds for a reply to the request.
- When the SBC receives a response to a policy request, it resumes sending requests for all traffic to Security Shield. You can define a list of three Cloud Communications Service (CCS) IP addresses. The SBC will attempt to connect to Security Shield starting with the CCS at the top of the list and if that is unsuccessful it attempts connection establishment by way of the next one on the list. Only when all three CCS connections do not respond will the SBC follow the process starting with the first bullet above.

Scenarios for Enabling or Disabling Mid-Call Updates

Sometimes you might want the Oracle® Communications Security Shield Cloud Service (Security Shield) to reassess calls and make mid-call updates to change the enforcement action, which might result in call termination. Or, you might not want the Security Shield to make mid-call updates because you want to avoid call termination. The following scenarios explain the circumstances and reasons.

Scenario for Enabling Mid-Call Updates

In the Cloud Communication Service (CCS) Installation procedure, the Activation script provides the option to use a WAN server certificate and WAN server private key that you supply. When you specify the WAN server certificate and WAN server private key parameters in the Activation script configuration, Security Shield enables mid-call updates.

When you enable mid-call updates, Security Shield uses port 443. If you specify some other port (other than 9000) CCS will use the specified port and allow mid-call updates. See the next scenario for port 9000 behavior.

> **Note:**
>
> If you change the CCS public IP address (WAN interface), it may take up to twenty four hours for mid-call updates to resume.

Scenario for Disabling Mid-Call Updates

Mid-call updates that occur after the SBC continues call processing may affect calls in progress, for example, calls answered by an Interactive Voice Response (IVR) system, a call agent, an employee, or a customer. Depending on your configuration, the typical mid-call update might terminate the call. Such termination can occur without warning causing agent dissatisfaction, customer dissatisfaction, and possible compliance issues. When regulatory compliance reasons do not allow you to block calls, Oracle recommends that you disable mid-call updates.

Disabling mid-call updates does not stop Security Shield from reassessing calls based on new information. In scenarios where mid-call updates are disabled and Security Shield reassess the call, the resulting action is to allow the call. The Security Shield Dashboard shows the reassessed results and the analytics reports, always providing the latest findings per call.

In the Cloud Communication Service (CCS) installation procedure, the Activation script provides the option to use a WAN server certificate and WAN server private key that you supply. When you leave the WAN server certificate and WAN server private key parameters empty in the Activation script configuration, Security Shield disables mid-call updates.

> **Note:**
>
> When you disable mid-call updates, Security Shield uses port 9000. If you specify some other port, CCS will use the specified port and allow mid-call updates. CCS will not disable mid-call updates when you specify a port other than 9000.

See "Enable or Disable Mid-Call Updates" in the *Security Shield Installation and Maintenance Guide*.

About Disabling Mid-Call Updates

In the Cloud Communication Service (CCS) installation procedure, the Activation script provides the option to use a WAN server certificate and WAN server private key that you supply. When you leave the WAN server certificate and WAN server private key parameters empty in the Activation script configuration, Oracle® Communications Security Shield Cloud Service(Security Shield) disables mid-call updates.

Note:

When you disable mid-call updates, Security Shield uses port 9000. If you specify some other port, CCS will use the specified port and allow mid-call updates. CCS will not disable mid-call updates when you specify a port other than 9000.

See "Enable or Disable Mid-Call Updates" in the *Security Shield Installation and Maintenance Guide*.

3

Inbound Call Labeling

Oracle® Communications Security Shield Cloud Service (Security Shield adds the P-OCSS-Call-Info header to the SIP INVITE when an inbound call passes through (Security Shield). The information in the header can improve call labeling, which can help you make more informed decisions about your call traffic.

Topics:

About Inbound Call Labeling

Oracle® Communications Security Shield Cloud Service (Security Shield) inbound call labeling can help you make call routing decisions.

Call Routing Uses

You might use the information in the P-OCSS-Call-Info header to

- route calls to the correct queue, such as a call agent, and select the appropriate Interactive Voice Response (IVR) menu for inbound calls.
- route a higher risk caller to a menu with restricted options, such as the ability to pay an outstanding bill but not the ability to change account information.
- route a call from a mobile phone to an IVR menu optimized for mobile calls, such as a shorter, reduced number of selections.
- route certain call-types through an additional verification step.

Behavior Notes

- After receiving a mid-call update, the Oracle Communications Session Border Controller (SBC) does not add any of the call-info parameter information to a SIP message.
- Security Shield removes the P-OCSS-Call-Info header from outbound SIP messages on untrusted realms.
- Security Shield captures configuration changes to call labeling in the Activity Log.
- The ci-key contains the SessionID that Security Shield generates, which you can use to view more details about the call in the Call Traffic Analytics Display Operations. The SessionID metric is in the Policy Results Statistics Attributes group.

P-OCSS-Call-Info Header Element Descriptions

The P-OCSS-Call-Info Header contains parameters that specify the type of information available for calls that pass through Oracle® Communications Security Shield Cloud Service (Security Shield). The header requires `Source` and `key`. The other elements are optional.

The P-OCSS-Call-Info header contains the following parameters and values.

> **Note:**
>
> The order of parameters that you see may vary from the following example.

```
label-info-params = [ci-reputation-score] / [ci-category] / [ci-
type] / [ci-device] / [ci-callerid-attest] / ci-source / ci-key
ci-score = "Reputation Score calling number" EQUAL 1*3DIGIT
ci-source = "origin" EQUAL "OCSS"ci-category = category EQUAL
("critical-risk" / "high-risk" / "severe-risk" / "significant-risk" /
"suspicious" / "good" / "trusted" /"acceptable" / "verified")
ci-callIerid-attest = "calledID-attest" EQUAL ( "trusted" /
"verified" / "not-verified"/ "failed")
ci-type = "type" EQUAL ("fraud-risk" / "spam-risk" / "call-center-
call" / "spoofed-call")
ci-device = "device" EQUAL ("FIXED_LINE" / "MOBILE”/ "OTHER" /
"PAGER" / "PAYPHONE" / "PERSONAL" / "RESTRICTED_PREMIUM" / "PREPAID" /
"TOLL_FREE" / VOICEMAIL" / "VOIP" / “INVALID”/ “HIGH_RISK”)
ci-key = "key" EQUAL "sessionID"
```

The following table lists and describes the header parameters.

Header Element	Description
source	(Required) Specifies Security Shield as the source of the data in this header. When the source is not available at the time of header creation, the header does not include this element.
key	(Required) Includes the unique call ID generated by Security Shield. This unique call ID allows for correlating call records between Security Shield and other systems.
category	(Optional) Specifies the call categories. See the Security Shield documentation for more information about the call categories. When the call category is not available at the time of the header creation, the header does not include this element. The header also supports the following values. • Trusted: Assigned when the call category equals Good and the STIR/SHAKEN indicator TN-Verstat Passed is received for this call. • Verified: Assigned when the call category equals Acceptable and the STIR/SHAKEN indicator TN-Verstat Passed is received for this call.

Header Element	Description
callerid-attest	(Optional) Specifies the trust level of the calling number. This information is based on the STIR/SHAKEN information provided by the Service Provider or SIP Trunk provider and the call category. Valid values: Trusted (reserved for future use) | Verified | Failed | Not Verified.
type	(Optional) Specifies the type of suspicious or potentially fraudulent call. When the type information is not available at the time of the header creation, he header does not include this element.
device	(Optional) Specifies the device or line type associated with the calling number. When the device information is not available at the time of the header creation, the header does not include this element. See "P-OCSS-Call-Info Codes, Types, and Values" for information about how to interpret the codes from the INVITE headers.
score	(Optional) Specifies the Reputation Score that Security Shield determined for the Calling Number.

The following example shows an INVITE configured for source, type, score, and key after passing through Security Shield from the Session Border Controller.

> **Note:**
>
> The order of parameters that you see may vary from the following example.

```
INVITE Request

       INVITE sip:alice@example.com SIP/2.0
       ...
       P-OCSS-Call-Info:
         ;source=OCSS ;category=severe-risk
         ;type=spam-risk ;device=voip
         ;score=41
         ;key=eyJzaXBUaHJlYWRJZCI6MywiY2FsbElkIjoid2xzcy1kNmNlNDczMi01NjYyODI
yNl82NzAzOTc4M0AxNTIuMTg4LjI1MS4xNDIiLCJmcm9tVGFnIjoiNmVjNzRjYjEiLCJ0aW1lc3Rh
bXAiOiIyMDIyLTAxLTEyVDIwOjExOjAwLjAxMFoiLCJzYmNJZCI6IlNCQ0xFQzYzNTBOQ0UwMUEiL
CJyZWFsbSI6InZ6X3dzYXRmXzAxX291dCJ9
```

P-OCSS-Call-Info Codes, Types, and Values

Oracle® Communications Security Shield Cloud Service (Security Shield) does not display the P-OCSS-Call-Info on the Dashboard. You must interpret the codes from the INVITE headers.

The following table lists the phone number type and name and ci-device value for each phone type code.

Number Type and Name	ci-device Supported Values
Fixed line number	FIXED_LINE
Mobile number	MOBILE
Other	OTHER
Pager	PAGER
Payphone number	PAYPHONE
Personal	PERSONAL
Restricted premium	RESTRICTED_PREMIUM
Prepaid (for prepaid mobile)	PREPAID
Toll-free number	TOLL_FREE
Voice mail number	VOICEMAIL
VOIP (non-fixed VOIP)	VOIP
Invalid	INVALID
High risk	HIGH_RISK

P-OCSS-Call-Info Header Codes

Oracle® Communications Security Shield Cloud Service (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.

Security Shield adds the header, as follows:

Table 3-1 P-OCSS-Call-Info Header Response Codes

Conditions	Status	Description
Full OCSS Response	200	Transaction successfully completed
No OCSS response	408	Request timeout
OCSS time-out	206	Transaction partially completed
No CSS connectivity	503	Service unavailable
Non-E164 Number (includes short numbers) Anonymous	422	Unprocessable entity

4

Phone Number Formatting

Oracle® Communications Security Shield Cloud Service (Security Shield) uses the E.164 phone number conventions. The following topics describe how to apply the conventions and how to handle nonconforming numbers.

Topics:

- Security Shield Phone Number Format Requirements
- How Security Shield Manages Nonconforming Calling Numbers
- Configure Nonconforming Number Handling

Security Shield Phone Number Format Requirements

Oracle® Communications Security Shield Cloud Service (Security Shield) requires the following conventions for phone numbers for inbound and outbound calls.

> **Note:**
>
> If your Session Border Controller does not use phone numbers in the E.164 format, Oracle may need to work with you before deploying Security Shield to determine how to normalize your phone numbers to work effectively with Security Shield.

- **Phone Number Format**
  The general number format convention is country code followed by the subscriber phone number <country code><subscriber phone number>. The subscriber phone number may include an area code and is typically seven to eleven digits long, depending on the national number conventions. Enter Phone numbers in the following ten-digit format where N is any digit from 2-9 (first digit of the area code and the local exchange) and X is any digit from 0-9: **NXX-NXX-XXXX** .

  > **Note:**
  >
  > The preceding example contains hyphens only to aid in understanding. Do not insert hyphens when entering the number in the "Number" field in the "Add Outbound Number" configuration.

- **Country Code**
  The country code can be up to three digits long. For international formatting, you may format the number with a + character (+<country code><subscriber phone number>, for example, +15551234567) or without the + character. For outbound calls to international destinations you can use either the + character or the international dialing prefix for your country. Check with your SIP trunk provider for the number format convention it supports. When formatting phone numbers for the Trusted Enterprise Calls subscription, which is valid only in North America, use one of the following methods to add the country code.

  - **Manual**—Add the +1 or 1 prefix to the number, for example +1NXXNXXXXXX or 1NXXNXXXXXX.
  - **Default to the United States and Canada**—Skip adding +1 or 1 to the number. Go to the Settings page and click Autonomous Threat Protection. Select "United States and Canada" for the "Service Domain Home Country." Security Shield will consider all phone numbers without a country code as "United States and Canada."
- You can use wild cards at the end of the phone number to indicate a range, except for Trusted Enterprise Calls. For example: To specify a seven digit phone number that begins with 91920, enter 91920xx.
- If you choose to configure the Presentation Number, you must use only the number format convention supported by the SIP trunk provider. When you use multiple SIP trunk providers, you must use a Presentation Number format that each SIP Trunk provider can support. For example, in the United States you use [country code][area code][local phone number] or the more commonly used [area code][local phone number]. In the European Union and United Kingdom you use [+][country code][area code][local phone number].

Number Cleansing

Use the following information to help you prepare phone numbers for Security Shield processing.

- Try to map to a country code to set the country.
- Remove any leading zeros from the phone number without the country code that may occur from configuration issues with trunk code or international dialing prefixes that are not removed.
- Map the next digits (prefix after the country code, after removing any leading zeros) to a carrier.
- Determine if the number length matches with the number plan (length for the prefix range.

When you receive calling number information (SIP INVITE, FROM, or PAI fields) containing a short phone number, incorrect format, or alphanumeric text such as "Restricted or "Anonymous", the reputation score may by negatively affected and can cause false positives for Reputation Score (High risk categories) and Threat Detection (Call Type). Oracle recommends that you use Security Shield Number Normalization, Non-Conforming E.641 Numbers guidelines, and Access Control Lists to avoid processing numbers with incorrect formats or alphanumeric text.

How Security Shield Manages Nonconforming Calling Numbers

When a calling number does not conform to E.164 phone number conventions, even after normalization, Oracle® Communications Security Shield Cloud Service (Security Shield) provides you with ways to specify call treatment.

A calling number that does not conform to E.164 phone number conventions may result from the following causes:

- The originating entity, originating Service Provider, or intermediate networks may have added the nonconforming phone number due to a configuration error, lack of validation, or incorrect or incomplete information. Some possible configuration errors include errors in one or more normalization rules, incorrect number length, or the number contains prefixes and suffixes. Typically, a nonconforming number seen in such scenarios is not malicious or ill-intended.

- A configuration error in the Number Normalization rules. This scenario is an error condition, and is not malicious by nature.
- Malicious use of nonconforming numbers to disguise the originator of the call or use of improperly formatted numbers to gain access or detect vulnerabilities. These are threat scenarios.

With any enforcement action other than Continue, Security Shield stops processing the call and performs the configured action. With Continue as the enforcement action, Security Shield continues call processing which includes the Access Control List and Threat Detection.

Reputation Score Call Classifications

Security Shield provides the following reputation score call classifications and scores for nonconforming calling numbers.

Low Risk—Security Shield successfully validated the caller's phone number and determined significant trust and confidence building activity. Examples of criteria include:

- Regular Call Activity
- Tenure (continuous long-term activity)
- Stable activity identified and the phone number is reachable

Medium Risk—Security Shield successfully validated the caller's phone number and detected medium risk activity. Examples of criteria include:

- Call Center-like activity
- Activity towards a high number of premium numbers
- Call duration (irregular call duration)
- Tenure (Sparse long-term activity or high short-term activity)
- Number types (Payphone, technical number,and virtual numbers)
- Probable Spam-risk calls
- When limited or no activity is detected for a phone number

High-Risk—Security Shield successfully validated the caller's phone number and detected high risk activity, the use of high-risk numbers or number types and reported fraudulent activity for the number. Examples of criteria include:

- Activity towards a high number of different phone numbers
- Activity towards a high number of unassigned phone numbers
- Tenure (no long-term activity or high short-term activity)
- Number types (High-risk and medium-risk carriers, high-risk phone type, high-risk prefix, high-risk country, toll free number, pager number, voice mail number, premium number, payphone, technical number, virtual number, or invalid number)
- Time bucket (Seen more than three months ago)
- Invalid phone number
- Traffic pumping
- Fraud risk, spoofed calls, or some Spam calls

Enforcement Actions

Security Shield provides the following enforcement actions that you can specify for nonconforming calling numbers.

Allow—(Default) Security Shield processes the calling number against your Access Control List and Threat Detection settings.

Block—Security Shield denies the call.

Redirect—Security Shield redirects the call to the number you specify.

Configure Nonconforming Number Handling

Oracle® Communications Security Shield Cloud Service (Security Shield) defaults to the Nonconforming Number call classification and the Continue enforcement action for nonconforming numbers. You can change the enforcement action from the Call Type Classifications page on the Settings page.

Before You Begin

- For more explanation of the parameters in the following procedure, see How Security Shield Manages Nonconforming Calling Numbers.

With any enforcement action other than Continue, Security Shield stops processing the call and performs the configured action. With Continue as the enforcement action, Security Shield continues call processing which includes the Access Control List and Threat Detection.

> **Note:**
>
> The classifications displayed for Call Type Classification depend on whether you own the Standard Edition or the Premium Edition.

1. Access the Settings page, and click **Call Type Classification**.
2. On the Call Type Classification page, set the enforcement action for the call type. Default: Continue. Valid values: Continue | Block | Redirect.
3. Click **Save**.

5

Common Controls and Actions

The Oracle® Communications Security Shield Cloud Service (Security Shield) provides a Web-based User Interface (UI) with pages where you can manage call traffic. The banner at the top of the UI is common to all Security Shield pages.

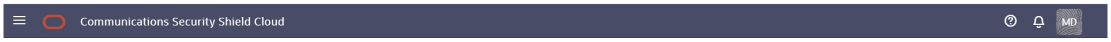
Topics:

- Descriptions of Common Controls and Actions

Descriptions of Common Controls and Actions

The following information describes the controls and actions that display at the top of every Oracle® Communications Security Shield Cloud Service (Security Shield) Web page.

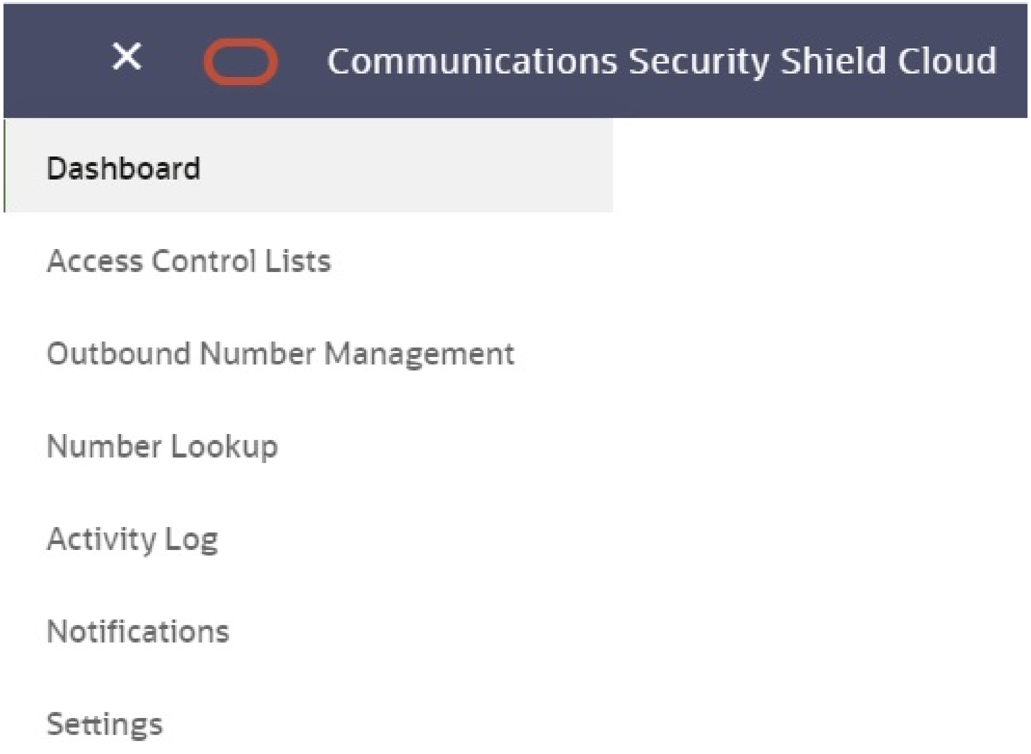
The banner displays the Navigation, Help, Notifications, and User menu icons.



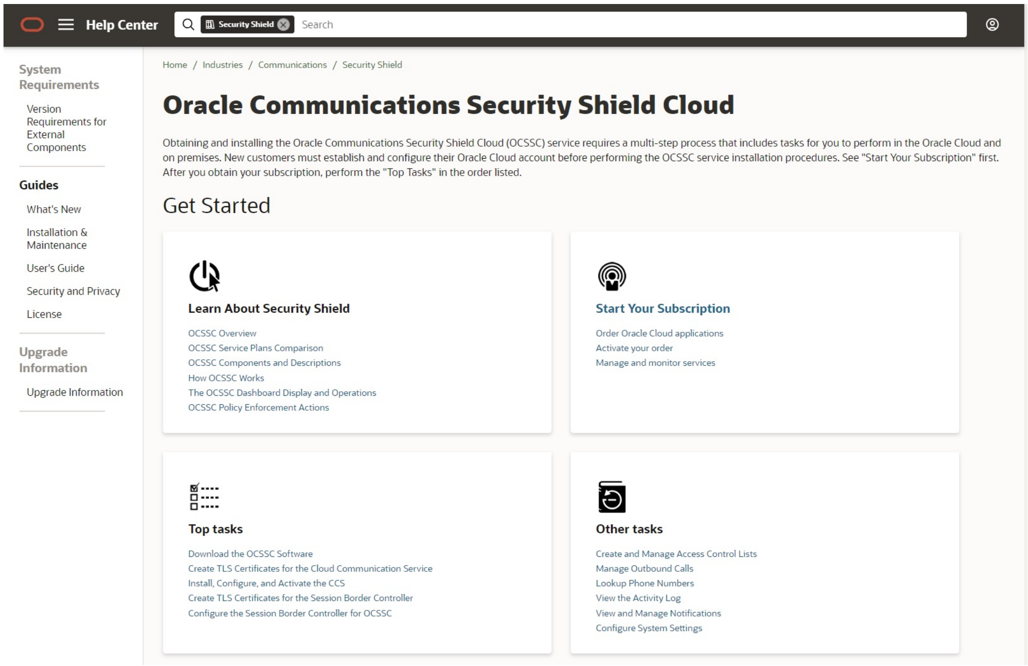
The following list describes the icons on the banner.

☰

Navigation Icon—Use to display a list of links to pages. For example,



Help Icon—Use to reach the Security Shield documentation. For example,

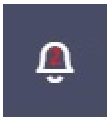


Oracle Communications Security Shield Cloud

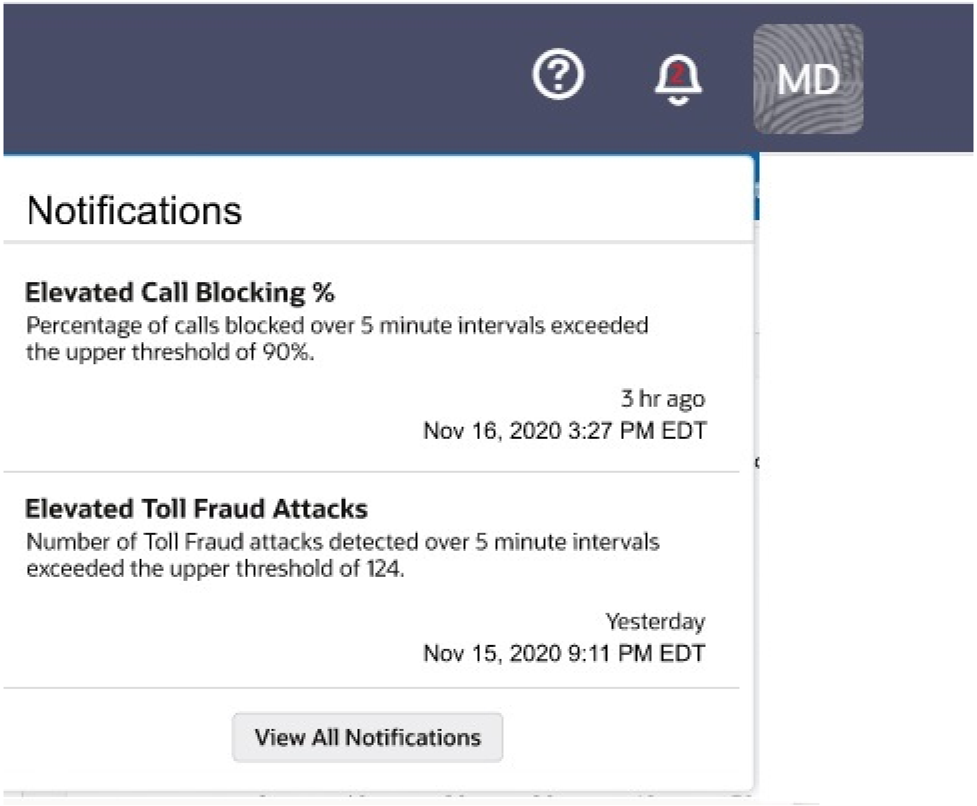
Obtaining and installing the Oracle Communications Security Shield Cloud (OCSSC) service requires a multi-step process that includes tasks for you to perform in the Oracle Cloud and on premises. New customers must establish and configure their Oracle Cloud account before performing the OCSSC service installation procedures. See "Start Your Subscription" first. After you obtain your subscription, perform the "Top Tasks" in the order listed.

Get Started

Learn About Security Shield
OCSSC Overview
OCSSC Service Plans Comparison
OCSSC Components and Descriptions
How OCSSC Works
The OCSSC Dashboard Display and Operations
OCSSC Policy Enforcement Actions
Start Your Subscription
Order Oracle Cloud applications
Activate your order
Manage and monitor services
Top tasks
Download the OCSSC Software
Create TLS Certificates for the Cloud Communication Service
Install, Configure, and Activate the CCS
Create TLS Certificates for the Session Border Controller
Configure the Session Border Controller for OCSSC
Other tasks
Create and Manage Access Control Lists
Manage Outbound Calls
Lookup Phone Numbers
View the Activity Log
View and Manage Notifications
Configure System Settings



Notifications Icon—Use to see a list of system notifications. When new notifications occur, the icon displays the count. For example,



Notifications

Elevated Call Blocking %

Percentage of calls blocked over 5 minute intervals exceeded the upper threshold of 90%.

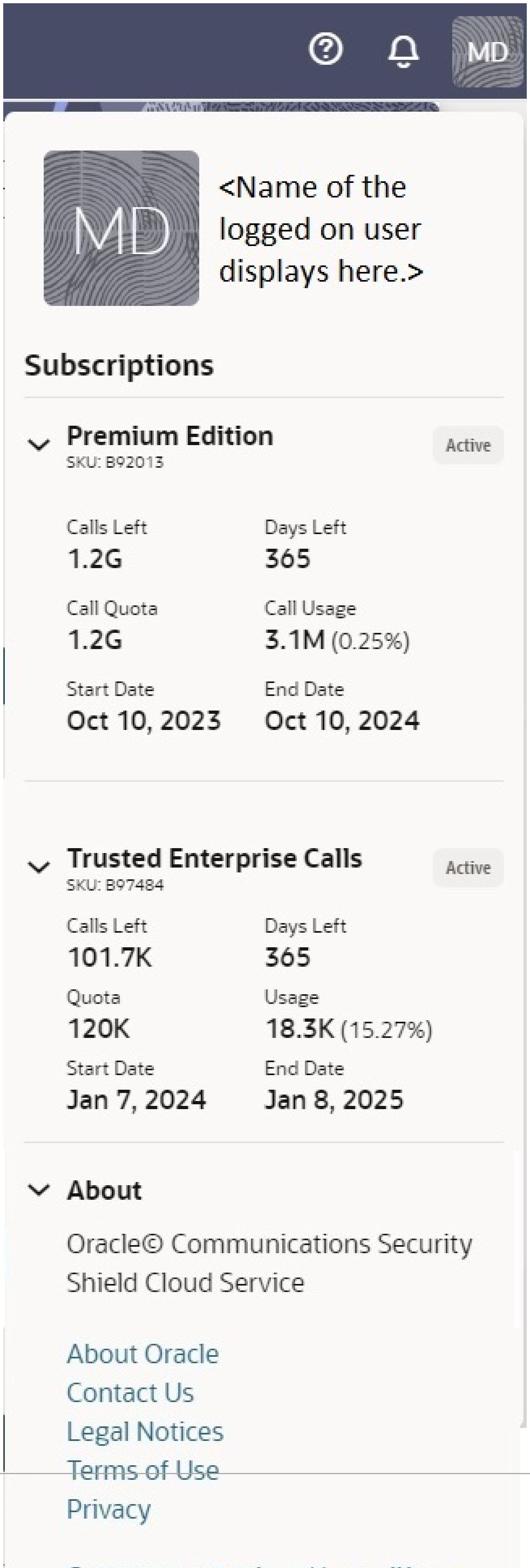
3 hr ago
Nov 16, 2020 3:27 PM EDT

Elevated Toll Fraud Attacks

Number of Toll Fraud attacks detected over 5 minute intervals exceeded the upper threshold of 124.

Yesterday
Nov 15, 2020 9:11 PM EDT

Avatar Icon—Use to see information about all of your subscriptions. Click the avatar with the user's initials to open the panel. The About section includes links to other product-related information.



<Name of the logged on user displays here.>

Subscriptions

Premium Edition Active

SKU: B92013

Calls Left 1.2G	Days Left 365
Call Quota 1.2G	Call Usage 3.1M (0.25%)
Start Date Oct 10, 2023	End Date Oct 10, 2024

Trusted Enterprise Calls Active

SKU: B97484

Calls Left 101.7K	Days Left 365
Quota 120K	Usage 18.3K (15.27%)
Start Date Jan 7, 2024	End Date Jan 8, 2025

About

Oracle© Communications Security Shield Cloud Service

About Oracle
Contact Us
Legal Notices
Terms of Use
Privacy

See the following topics for information about the controls and actions that are unique to each page.

- The Dashboard
- Access Control Lists
- Outbound Number Management
- Number Lookup
- Activity Logs
- Notifications
- Settings

6

The Dashboard

The Oracle® Communications Security Shield Cloud Service (Security Shield) Dashboard displays information about the SIP call traffic crossing your telephony network boundary and provides tools to help you manage its security. Some tools are interactive, where you can change certain settings from the Dashboard to quickly respond to traffic conditions. The Dashboard also reports on the state of your network devices, as well as the enforcement actions that the Security Shield applied according to the policies and thresholds you set.

Through the Dashboard, you can:

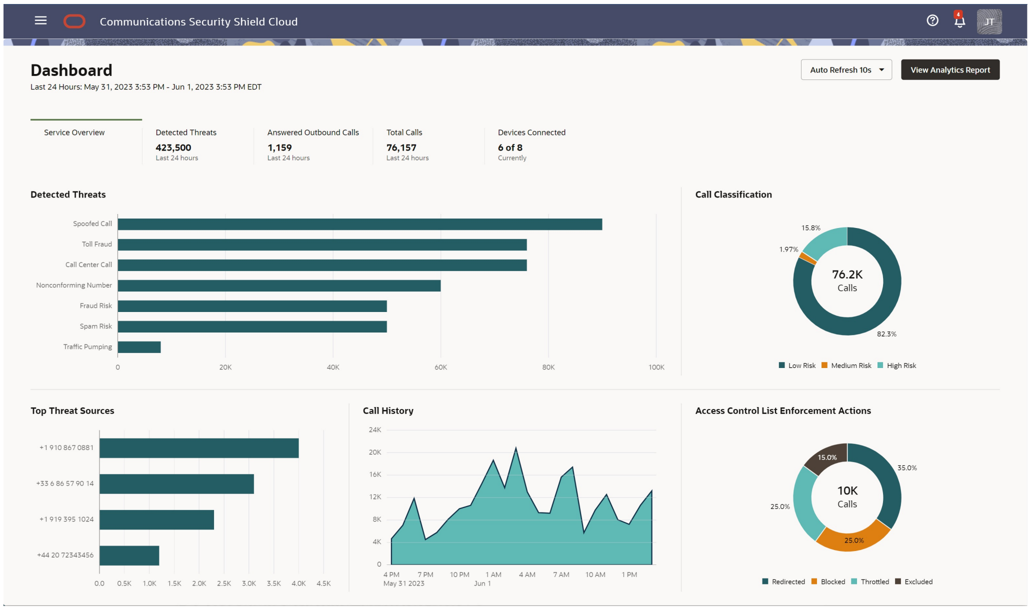
- View detected threats and take action on potential security threats and possible fraud, for example, by specifying thresholds on call activities.
- View specific details about calls that applied enforcement action, for example, blocked calls and re-directed calls.
- View and manage the status of connected devices such as the Session Border Controllers, for example, so you can see which devices are in and out of service.
- View metrics about answered trusted outbound enterprise calls.
- View details about your subscriptions, such as usage and expiration dates.

Topics:

Dashboard Controls and Actions

The Dashboard displays tabs with visual representations of information about Oracle® Communications Security Shield Cloud Service (Security Shield) services and call traffic crossing your telephony network boundary. The information reflects recent activity and refreshes each time you access the Dashboard and periodically refreshes as configured with the Auto Refresh setting.

The tabs on the Dashboard provide you with a complete view of how, why, and when Security Shield protected your telephony network within the last 24 hours. The following screen capture shows an example of the Dashboard including the Answered Outbound Calls scoreboard tab that displays with the optional Trusted Enterprise Calls subscription.



Last 24 Hours: May 31, 2023 3:53 PM - Jun 1, 2023 3:53 PM EDT

Service Overview

Detected Threats
423,500
Last 24 hours

Answered Outbound Calls
1,159
Last 24 hours

Total Calls
76,157
Last 24 hours

Devices Connected
6 of 8
Currently

Auto Refresh—While viewing the dashboard, the refresh rate depends on the setting you configure for auto-refresh. To refresh the data while viewing the dashboard, rather than re-launching the dashboard to force the update, you can set the refresh rate at 10, 30, 60, or 90 seconds with the Auto Refresh control. The default is every 10 seconds.

View Analytics Report—When you want to investigate your inbound and outbound call traffic, as well as anomalies, suspicious behavior, and malicious traffic, click Analytics Report.

Last 24 Timestamp—The 24-hour period for which the Dashboard displays data. The Dashboard uses the local date and time where the browser is launched.

Metrics Cards—The Service Overview tab displays interactive metrics cards that provide key performance indicators. When you hover over certain areas of the metrics cards, the Dashboard displays more granular data. The available metric cards depend on the subscription you purchase.

- When you purchase the Trusted Enterprise Calls subscription with either the Standard or Premium subscription, Security Shield adds the Answered Outbound Calls metrics card to the Dashboard along with the others.
- When you purchase only the Trusted Enterprise Calls subscription, the Dashboard displays only the Answered Outbound Calls and Devices Connected metrics cards. Security Shield hides the others.

> **Note:**
>
> No data displays on the Dashboard until you connect the on-premises devices and the Security Shield service starts processing calls.

See the following topics for descriptions of the Key Performance Indicator scoreboards on the Dashboard.

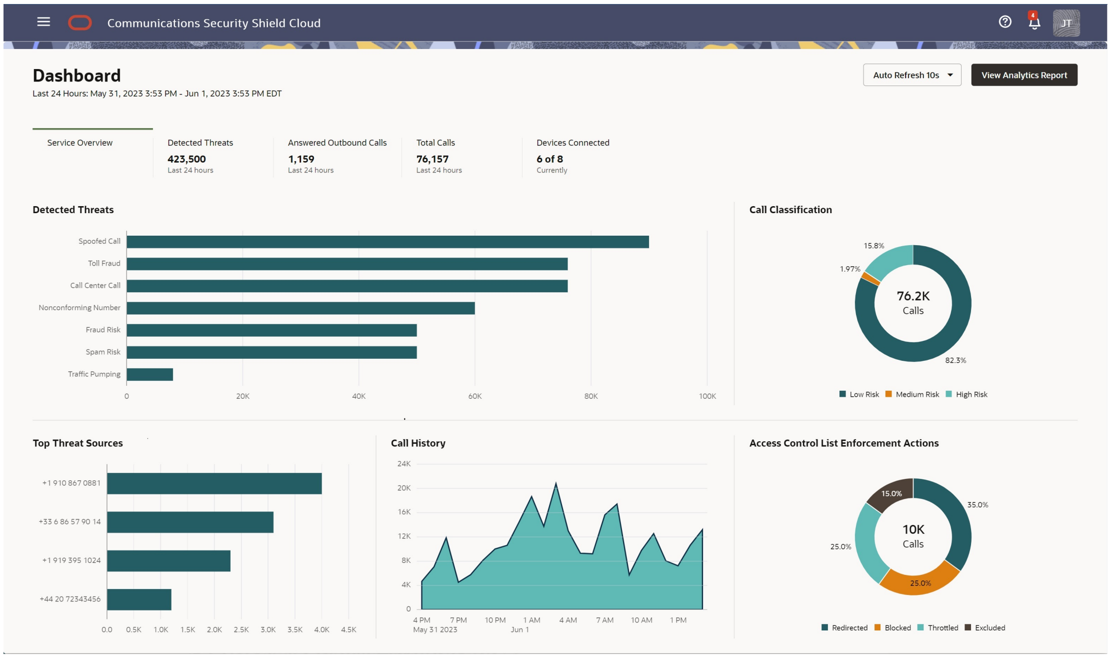
- The Service Overview Scoreboard

- The Detected Threats Scoreboard Metrics Card
- The Answered Outbound Calls Scoreboard Metrics Card
- The Total Calls Scoreboard Metrics Card
- The Devices Connected Scoreboard Metrics Card

The Service Overview Scoreboard

The Oracle® Communications Security Shield Cloud Service (Security Shield) Service Overview scoreboard displays charts and graphs showing the state of call traffic in your telephony network within the last twenty-four hours.

The following screen capture shows an example of the Service Overview scoreboard with data.



Communications Security Shield Cloud

Dashboard

Last 24 Hours: May 31, 2023 3:53 PM - Jun 1, 2023 3:53 PM EDT

Service Overview	Detected Threats	Answered Outbound Calls	Total Calls	Devices Connected
	423,500 Last 24 hours	1,159 Last 24 hours	76,157 Last 24 hours	6 of 8 Currently

Detected Threats—Shows the number of threats per threat type such as Toll Fraud, Traffic Pumping, Fraud Risk, Spam Risk, Call Center Call, Spoofed Call, Non-conforming Number, High Risk, and Medium Risk calls.

Call Classifications—Shows the number of threats per call classification type such as Low Risk, Medium Risk, and High Risk.

Top Threat Sources—Shows the phone numbers of the top sources of threats in the categories of Allowed, Throttled, Blocked, and Redirected calls.

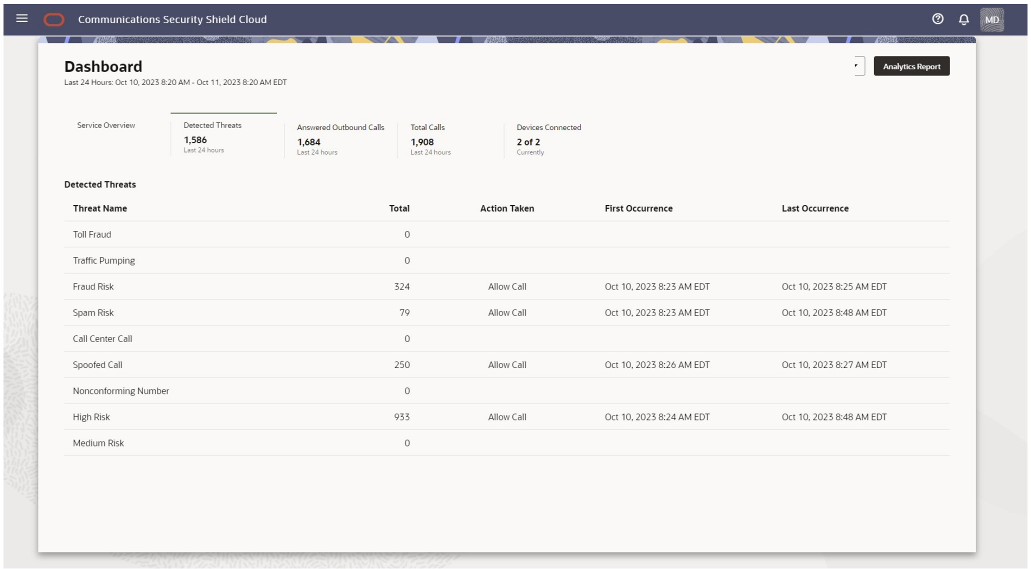
Call History—Shows the total numbers of calls processed in the last twenty four hours. You can hover over a particular point in time to see more details.

Access Control List Enforcement Actions—Shows the number of calls affected by your Access Control Lists, such as Throttled, Blocked, Redirected, and Excluded calls. When you hover over a section of the chart, the system shows the action taken and the number of call actions for the type.

The Detected Threats Scoreboard Metrics Card

The Detected Threats scoreboard metrics card shows the total number of threats Oracle® Communications Security Shield Cloud Service (Security Shield) detected in the last twenty-four hours. The card displays a breakdown of the number of each threat type detected along with the last action taken and the date and time of the first and last occurrence.

The following screen capture shows the Premium Subscription Detected Threats scoreboard metrics card with sample data.



Dashboard

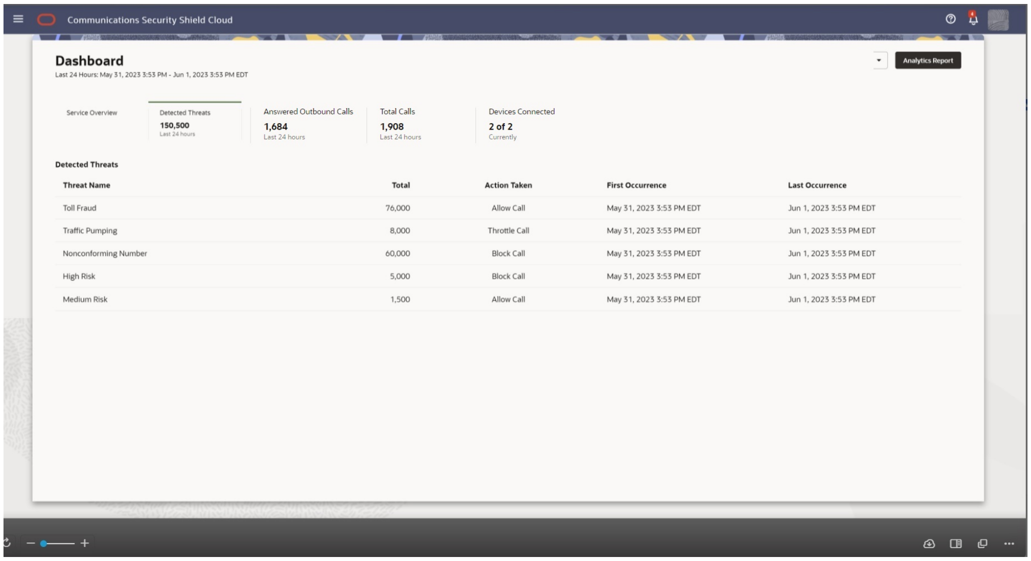
Last 24 Hours: Oct 10, 2023 8:20 AM - Oct 11, 2023 8:20 AM EDT

Service Overview	Detected Threats	Answered Outbound Calls	Total Calls	Devices Connected
	1,586 Last 24 hours	1,684 Last 24 hours	1,908 Last 24 hours	2 of 2 Currently

Detected Threats

Threat Name	Total	Action Taken	First Occurrence	Last Occurrence
Toll Fraud	0			
Traffic Pumping	0			
Fraud Risk	324	Allow Call	Oct 10, 2023 8:23 AM EDT	Oct 10, 2023 8:25 AM EDT
Spam Risk	79	Allow Call	Oct 10, 2023 8:23 AM EDT	Oct 10, 2023 8:48 AM EDT
Call Center Call	0			
Spoofed Call	250	Allow Call	Oct 10, 2023 8:26 AM EDT	Oct 10, 2023 8:27 AM EDT
Nonconforming Number	0			
High Risk	933	Allow Call	Oct 10, 2023 8:24 AM EDT	Oct 10, 2023 8:48 AM EDT
Medium Risk	0			

The following screen capture shows the Standard Subscription Detected Threats scoreboard metrics card with sample data.



Dashboard

Last 24 Hours: May 31, 2023 3:53 PM - Jun 1, 2023 3:53 PM EDT

Service Overview	Detected Threats	Answered Outbound Calls	Total Calls	Devices Connected
	150,500 Last 24 hours	1,684 Last 24 hours	1,908 Last 24 hours	2 of 2 Currently

Detected Threats

Threat Name	Total	Action Taken	First Occurrence	Last Occurrence
Toll Fraud	76,000	Allow Call	May 31, 2023 3:53 PM EDT	Jun 1, 2023 3:53 PM EDT
Traffic Pumping	8,000	Throttle Call	May 31, 2023 3:53 PM EDT	Jun 1, 2023 3:53 PM EDT
Nonconforming Number	60,000	Block Call	May 31, 2023 3:53 PM EDT	Jun 1, 2023 3:53 PM EDT
High Risk	5,000	Block Call	May 31, 2023 3:53 PM EDT	Jun 1, 2023 3:53 PM EDT
Medium Risk	1,500	Allow Call	May 31, 2023 3:53 PM EDT	Jun 1, 2023 3:53 PM EDT

Note:

The Answered Outbound Calls tab displays only for Trusted Enterprise Calls subscribers.

Threat Descriptions

Toll Fraud—Indicates that perpetrators accessed a company's phone lines then used those lines to call premium rate numbers that they have set up. The unsuspecting company must pay the bill. (Standard and Premium)

Traffic Pumping—Indicates calls that exceeded the configured upper threshold of the call attempt rate for five minutes. (Standard and Premium)

Fraud Risk—Indicates high-risk unwanted calls likely originating from entities posing as legitimate callers with malicious intent, such as to defraud you. This is not a call from a Fraud Risk department. (Premium) Security Shield classified the call as a fraud risk, due to association with known scams or dangerous activity. Administrators typically set the enforcement action to Redirect Call for advanced authentication or Block.

Spam Risk—Indicates Spam or other unwanted calls from suspect phone numbers, such as phone numbers that originate large numbers of robocalls. Security Shield classified the call as Spam, due to the caller's patterns indicative of spam calls. Administrators typically set the enforcement action to Block. (Premium)

Call Center Call—Indicates wanted call notifications from direct marketers of goods and services to potential customers. Such calls include verification codes, appointment reminders, school announcements, and so on. Security Shield classified the call as a Call Center Call, due to potential value to the recipients. Administrators typically set the enforcement action to Continue. (Premium)

Spoofed Call—Indicates calls originating from an entity that disguised the caller's identity, hijacked the phone number, used a recently unassigned phone number, and other calls that do not fit into the other classifications. For example, an incorrectly entered phone number might classify as a Spoofed Call. Administrators typically set the enforcement action to Block. (Premium)

Nonconforming Number—Indicates the calling number does not conform to E.164 conventions after number normalization. Possible reasons include errors in one or more normalization rules, incorrect number length, or the number contains prefixes and suffixes. A nonconforming number might also indicate a threat. (Standard and Premium)

High Risk—Indicates that there is no long-term activity and there is activity towards a high number of different phone numbers and unassigned phone numbers. Significant risk factors also include no long-term activity and high short-term activity. (Standard and Premium)

Medium Risk—Indicates activity that is call center-like, sparse, directed towards a high number of premium numbers, or comes from a high number of toll-free numbers. Significant risk factors also include a high number of completed calls and irregular call duration. (Standard and Premium)

Enforcement Actions Taken Descriptions

Block Call—Stops the call from proceeding.

Redirect Call—Directs the call to a number you specify in the Access Control List rule.

Throttle—Limits the number of calls from the selected calling and called numbers on the list by allowing only the configured percentage of calls. For example, you might want to throttle international calls to limit such expensive calls beyond the threshold you set. You can configure the percentage of outbound calls to throttle for each number on the list through the Add Number and Edit Number Attributes dialogs. When Security Shield throttles a particular phone number, the system chooses the calls to block to that number in a random manner such that overall percentage of calls allowed matches the configured percentage.

> **Note:**
>
> You might see some fluctuation where the actual value sometimes differs from the configured value.

Exclude—Allows inbound calls while still evaluating against Traffic Pumping, Spoofing, and Toll Fraud threat detection. Exclude ignores the risk assessment and classifies excluded calls as "Good". The Exclude action does not evaluate against Fraud Risk, Spam Risk, and Call Center call detection.

Allow—Allows the call to proceed under the following conditions:

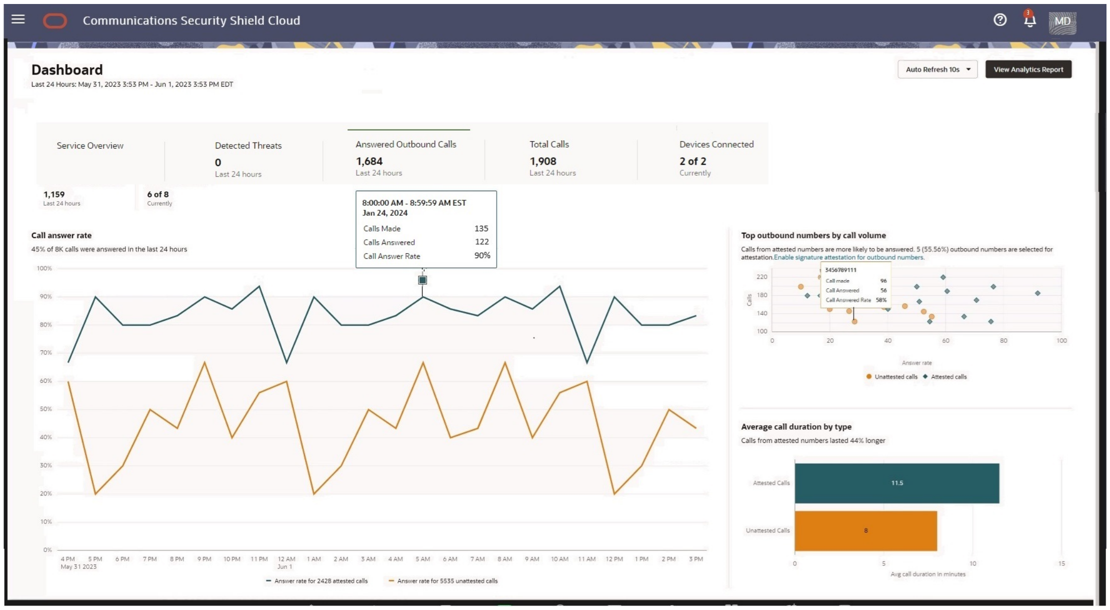
- When the Access Control List enforcement action is set to Allow, Security Shield allows the call regardless of the enforcement action set for the reputation score.
- When the response code from the call look-up is anything but Continue, Security Shield performs the specified action.
- When the response code from the call look-up is set to Continue, the call type is reported and no call enforcement is associated with this detection. Call enforcement depends on other threats detected or the reputation score enforcement and associated settings.

> **Note:**
>
> When there is a conflict between the Call Classification Type action and the Reputation Score Classification action, the Call Classification Type setting takes precedence.

The Answered Outbound Calls Scoreboard Metrics Card

Oracle® Communications Security Shield Cloud Service (Security Shield) adds the Answered Outbound Calls scoreboard metrics card to the Dashboard when you purchase the Trusted Enterprise Calls subscription. The tab displays charts and graphs showing metrics about your attested and unattested outbound calls.

The following screen capture shows the Answered Outbound Calls scoreboard metrics card with sample data.



Communications Security Shield Cloud

Dashboard

Last 24 Hours: May 31, 2023 3:53 PM - Jun 1, 2023 3:53 PM EDT

Service Overview

1,159
Last 24 hours

6 of 8
Currently

Detected Threats
0
Last 24 hours

Answered Outbound Calls
1,684
Last 24 hours

Total Calls
1,908
Last 24 hours

Devices Connected
2 of 2
Currently

Call answer rate

45% of 8K calls were answered in the last 24 hours

8:00:00 AM - 8:59:59 AM EST
Jan 24, 2024

Calls Made	135
Calls Answered	122
Call Answer Rate	90%

Top outbound numbers by call volume

Calls from attested numbers are more likely to be answered. 5 (55.56%) outbound numbers are selected for attestation.Enable signature attestation for outbound numbers.

3456789111

Call made	96
Call Answered	56
Call Answered Rate	58%

Average call duration by type

Calls from attested numbers lasted 44% longer

Graph Descriptions

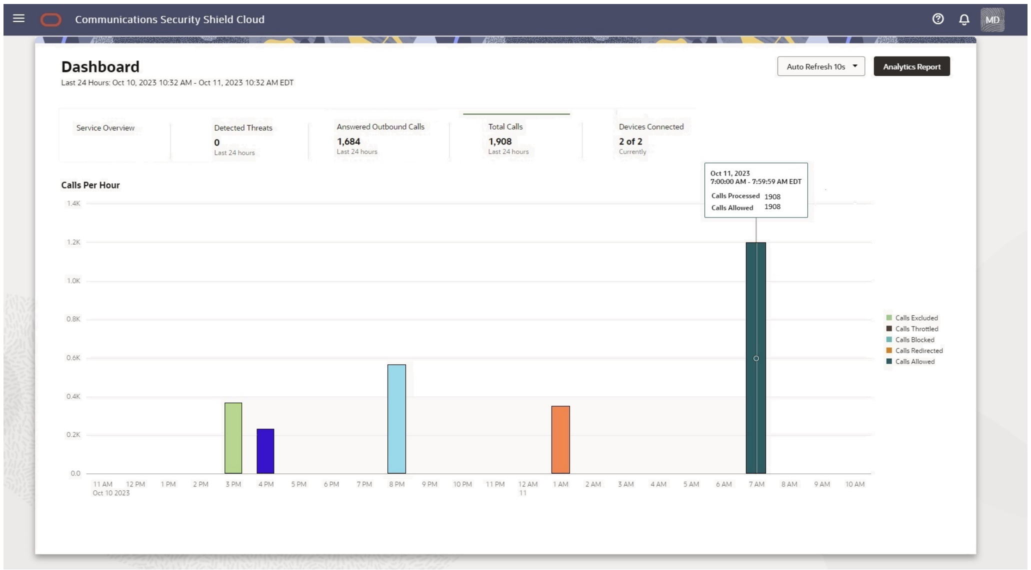
Call Answer Rate—Shows the percentage of the number of outbound calls that were answered in the last twenty-four hours. One line shows the answer rate for attested calls and the other line shows the answer rate for unattested calls. When you hover over any point in time on either line, Security Shield displays the timestamp, number of calls made, number of calls answered, and the call answer rate.

Top Outbound Numbers by Call Volume—Shows the top fifteen attested and unattested outbound phone numbers used in the last twenty-four hours. When you hover over a call bubble (round for unattested calls and diamond shaped for attested calls), Security Shield displays the number of calls made from the selected number, the number of those calls that were answered, and the call answer rate. To enable an unattested phone number for attestation, click the "Enable signature attestation for outbound numbers" link. Security Shield displays the Outbound Number Management page where you can enable the phone number for call signing and attestation. Security Shield logs the change in the Activity Log.

Average Call Duration by Type—Shows the duration of attested and unattested calls in minutes and how much longer attested calls lasted than unattested calls.

The Total Calls Scoreboard Metrics Card

The Total Calls scoreboard metrics card displays the total number of calls that passed in and out of your telephony network in the last twenty-four hours. When you hover over a time on the horizontal axis, the system displays information about the type of calls received for the time period.



Dashboard

Last 24 Hours: Oct 10, 2023 10:32 AM - Oct 11, 2023 10:32 AM EDT

Service Overview

Detected Threats 0 Last 24 hours

Answered Outbound Calls 1,684 Last 24 hours

Total Calls 1,908 Last 24 hours

Devices Connected 2 of 2 Currently

Oct 11, 2023
7:00:00 AM - 7:59:59 AM EDT
Calls Processed 1908
Calls Allowed 1908

> **Note:**
>
> The Answered Outbound Calls tab displays only for Trusted Enterprise Calls subscribers.

Call Total Descriptions

Calls Excluded—The number of inbound calls allowed while still evaluating against Traffic Pumping, Spoofing, and Toll Fraud threat detection. Exclude ignores the risk assessment and classifies excluded calls as "Good". The Exclude action does not evaluate against Fraud Risk, Spam Risk, and Call Center call detection.

Calls Throttled—The number of calls allowed from specified calling and called numbers on the Access Control List per the percentage you set to limit such calls.

Calls Blocked—The number of calls blocked.

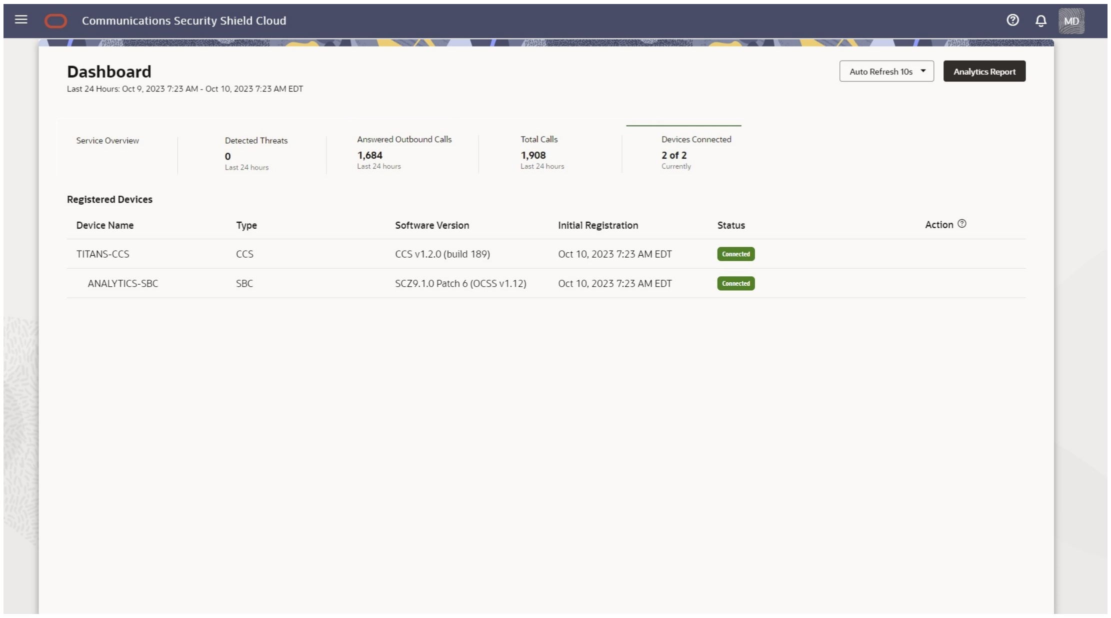
Calls Redirected—The number of calls redirected to a specified number.

Calls Allowed—The number of calls allowed.

The Devices Connected Scoreboard Metrics Card

The Devices Connected scoreboard metrics card lists your devices connected to Oracle® Communications Security Shield Cloud Service (Security Shield) and information about their status.

The following screen capture shows the Devices Connected scoreboard metrics card with sample data.



Dashboard

Last 24 Hours: Oct 9, 2023 7:23 AM - Oct 10, 2023 7:23 AM EDT

Service Overview	Detected Threats	Answered Outbound Calls	Total Calls	Devices Connected
	0 Last 24 hours	1,684 Last 24 hours	1,908 Last 24 hours	2 of 2 Currently

Registered Devices

Device Name	Type	Software Version	Initial Registration	Status	Action
TITANS-CCS	CCS	CCS v1.2.0 (build 189)	Oct 10, 2023 7:23 AM EDT	Connected	
ANALYTICS-SBC	SBC	SCZ9.1.0 Patch 6 (OCSS v1.12)	Oct 10, 2023 7:23 AM EDT	Connected	

Note:

The Answered Outbound Calls tab displays only for Trusted Enterprise Calls subscribers.

Devices include the Cloud Communication Service (CCS) and the Oracle Communications Session Border Controller (SBC). When you configure a device, it automatically starts to register. Device Status also lists the software version running on each device, the date when the device initially registered, and actions taken.

The only interactive function provided is the ability to delete a device with the delete icon, which displays in the Action column. Before deleting a device, you must either take the device offline or disable the configuration that allows it to connect to Security Shield. If you do not, the device will re-register on its own, and will reappear in the device list. You cannot delete a parent device until you delete all of its child devices.

7

Access Control Lists

Oracle® Communications Security Shield Cloud Service (Security Shield) Access Control Lists allow you to configure rules and enforcement actions for inbound and outbound calling numbers and called numbers.

Topics:

Access Control Lists Controls and Actions

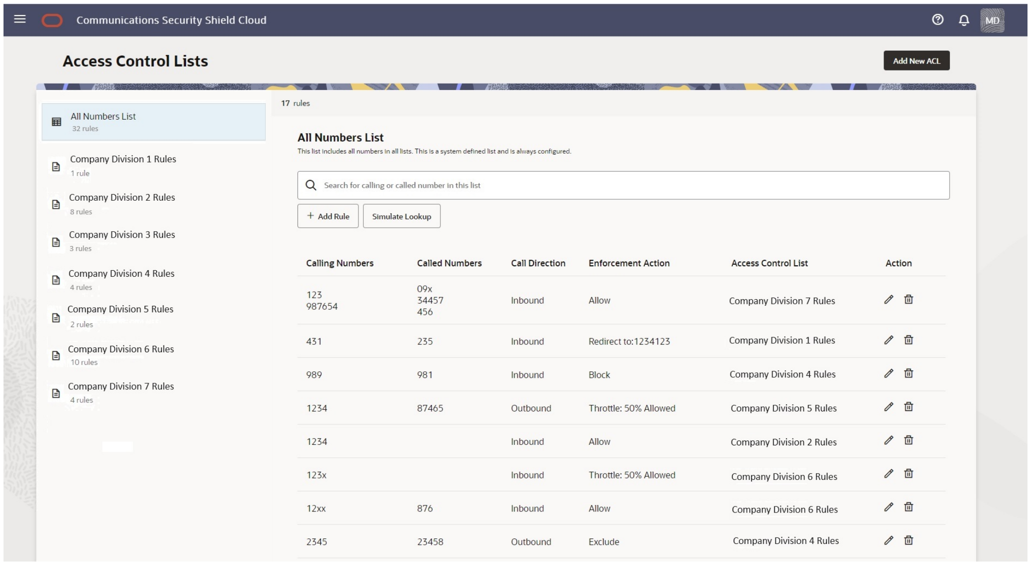
The Oracle® Communications Security Shield Cloud Service (Security Shield) Access Control Lists page displays lists of phone numbers and rules you create to control call traffic in and out of your telecommunications network. You can create lists for enterprise-wide control as well as for controlling calls to specific individuals or destinations.

The Access Control List page displays the system-generated All Rules List along with any lists you create in the left pane and the details of the lists in the right pane. The All Rules List is a summary view of all your access controlled phone numbers and rules.

When you add, edit, or delete rules on any of your user-created lists, the All Rules List updates accordingly. Likewise, when you add, edit, or delete a phone number on the All Rules List, Security Shield updates the user-created list that contains the rule and number. The Activity Log reports such changes.

> **Note:**
>
> You cannot rename or delete the All Rules List.

The following screen capture shows an example of the Access Control List page with the system-named All Rules List, and some user-created lists in the left pane and the details of the highlighted list in the right pane.



Access Control Lists

All Numbers List
32 rules

Company Division 1 Rules
1 rule

Company Division 2 Rules
8 rules

Company Division 3 Rules
3 rules

Company Division 4 Rules
4 rules

Company Division 5 Rules
2 rules

Company Division 6 Rules
10 rules

Company Division 7 Rules
4 rules

17 rules

All Numbers List

This list includes all numbers in all lists. This is a system defined list and is always configured.

Search for calling or called number in this list

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
123 987654	09x 34457 456	Inbound	Allow	Company Division 7 Rules	✎ 🗑
431	235	Inbound	Redirect to:1234123	Company Division 1 Rules	✎ 🗑
989	981	Inbound	Block	Company Division 4 Rules	✎ 🗑
1234	87465	Outbound	Throttle: 50% Allowed	Company Division 5 Rules	✎ 🗑
1234		Inbound	Allow	Company Division 2 Rules	✎ 🗑
123x		Inbound	Throttle: 50% Allowed	Company Division 6 Rules	✎ 🗑
12xx	876	Inbound	Allow	Company Division 6 Rules	✎ 🗑
2345	23458	Outbound	Exclude	Company Division 4 Rules	✎ 🗑

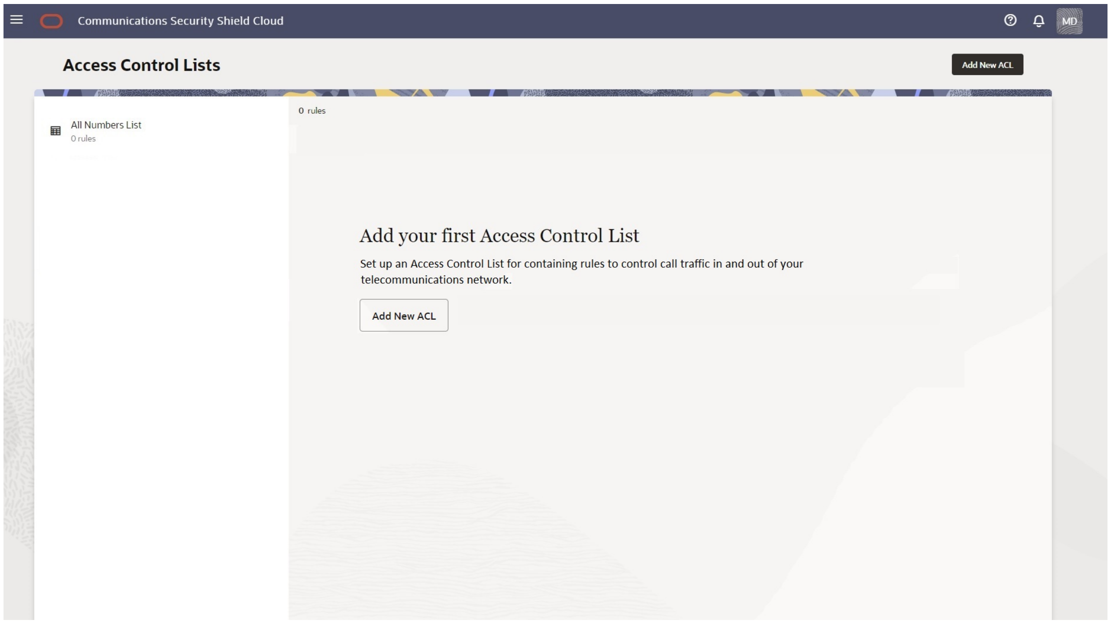
Use the **Add New ACL** button to add an Access Control list. You can add up to ten lists. When you reach the limit, the system deactivates the **Add New ACL** button. Each user-created list displays the edit and delete icons when you hover over the list name. For new customers, the Access Control List interface displays only the All Rules List, which is empty until you add lists. For upgrading customers, the system imports your preexisting access control lists and populates the All Rules List with the numbers from the imported lists.

The right pane displays the **Add Rule** button for adding new rules to user-created lists. Each rule on a list displays the edit and delete icons.

- When working with the All Rules List, the right pane displays the Search field and the Simulate Lookup button.
- When working with a user-created list, the right pane displays the Search field but not the Simulate Lookup button.

> **Note:**
>
> You may find that Search on the All Rules List is especially useful when you don't know which access control list contains a number you want to find because the search results identifies the list.

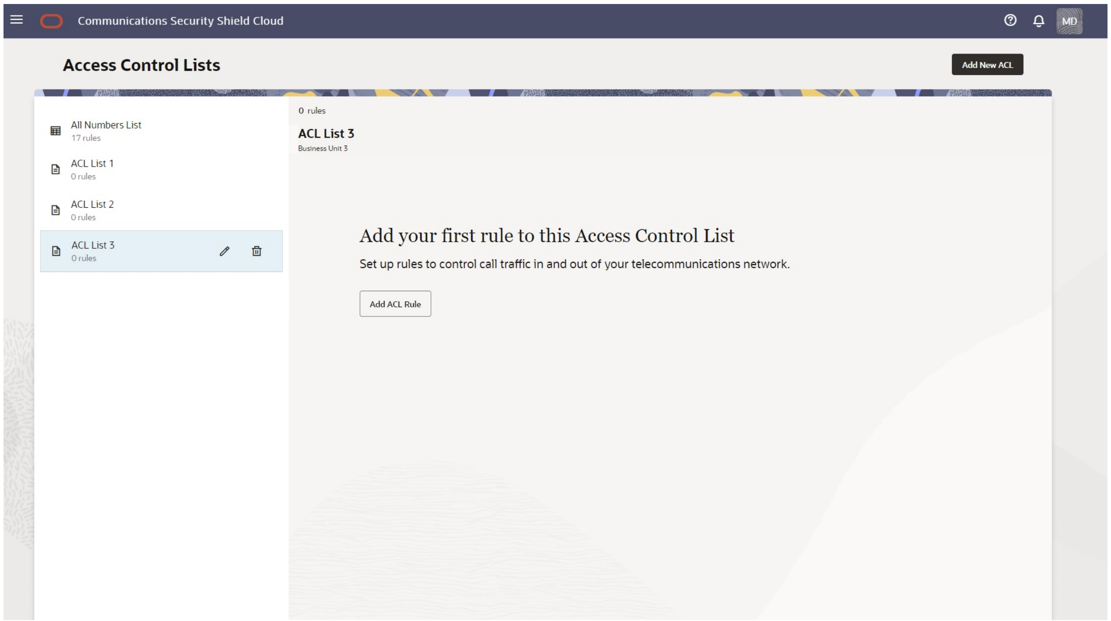
When no user-created Access Control lists exist, for example, when you first install Security Shield or when you delete all your user-created lists, Security Shield displays the message shown in the following screen capture. (Click **Add ACL List** to add a list.)



Add your first Access Control List

Set up an Access Control List for containing rules to control call traffic in and out of your telecommunications network.

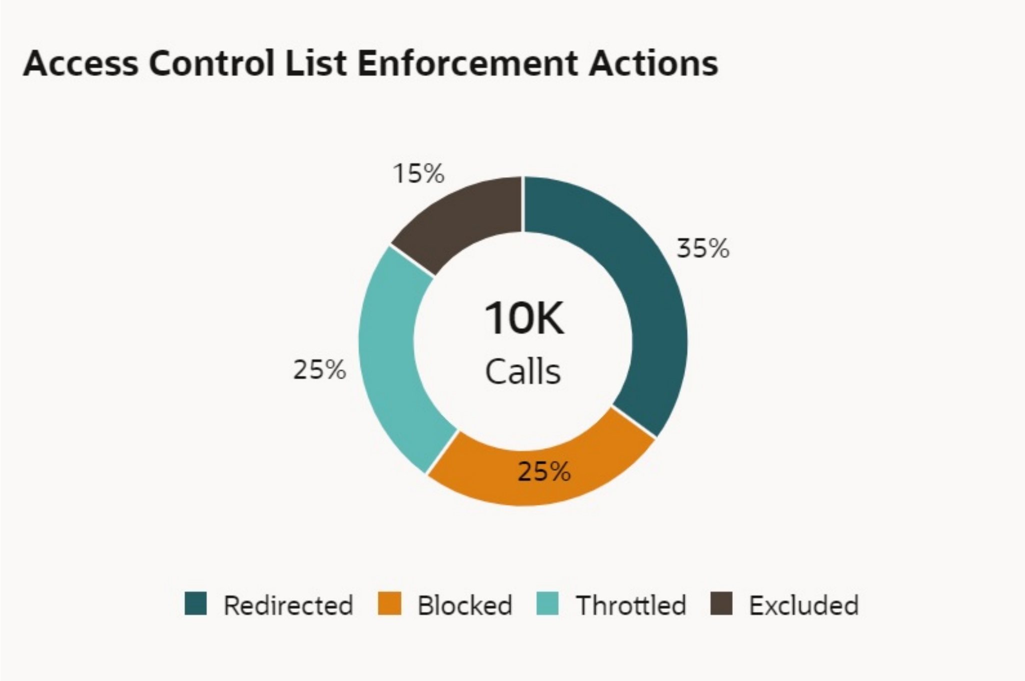
When a user-created Access Control list contains no rules, for example, when you first create the list or when you delete all the rules on the list, Security Shield displays the message shown in the following screen capture. (Click **Add ACL Rule** to add a phone number.)



Add your first rule to this Access Control List

Set up rules to control call traffic in and out of your telecommunications network.

When you create access control lists, the Security Shield reports their cumulative enforcement actions on the Access Control List Enforcement Actions tile on the Dashboard. The tile shows total number of inbound and outbound enforcement actions taken and displays a pie chart with the percent of actions taken per enforcement type. When you hover over a section of the pie chart, the tile shows the action taken and the number of call actions for the type.



Security Shield processes Access Control Lists (ACL) independently from regular threat processing and an action taken due to an ACL match over-rides decisions made due to threat analysis. Calls that match an ACL rule are also fully analyzed for threat status. The threat status is reported as part of the Security Shield Dashboard statistics and is also available in the analytics reports environment. The system reports both the ACL status and the threat status of the call.

About Access Control Lists and Upgrades

When Oracle upgrades Oracle® Communications Security Shield Cloud Service (Security Shield), the system migrates your preexisting access control lists with their preexisting names and rules.

In the upgrade process, Security Shield migrates you preexisting numbers configured for inbound to the Calling Number list and numbers configured for outbound to the Called Number list.

Access Control List Enforcement Actions

When you create an access control list rule, you must specify the enforcement action that you want Oracle® Communications Security Shield Cloud Service (Security Shield) to apply.

You can choose from the following enforcement actions for an access control list rule.

Allow —Allows inbound calls, but will evaluate the inbound call against Traffic Pumping, Spoofing, and Toll Fraud threat detection. Allow ignores the risk assessment and classifies the call as "Good". The Allow action does not evaluate the call against Fraud, Spam, and Call Center detection

Block —Blocks calls from the selected calling and called numbers on the list from proceeding in the specified direction.

Exclude—Allows inbound calls while still evaluating against Traffic Pumping, Spoofing, and Toll Fraud threat detection. Exclude ignores the risk assessment and classifies excluded calls as "Good". The Exclude action does not evaluate against Fraud Risk, Spam Risk, and Call Center call detection.

Redirect —Sends inbound calls from the selected calling and called numbers on the list to the destination that you specify. For example, you can route specific numbers with a history of fraudulent activity associated with them, or that come from specific international destinations, to a security desk for additional screening. All calls to a specific phone number go to the same specified redirect destination because Security Shield does not support redirecting to multiple locations per phone number. You can specify a redirect number per inbound phone number.

Throttle —Limits the number of calls from the selected calling and called numbers on the list by allowing only the configured percentage of calls. For example, you might want to throttle international calls to limit such expensive calls beyond the threshold you set. You can configure the percentage of outbound calls to throttle for each number on the list through the Add Number and Edit Number Attributes dialogs. When Security Shield throttles a particular phone number, the system chooses the calls to block to that number in a random manner such that overall percentage of calls allowed matches the configured percentage.

> **Note:**
>
> You might see some fluctuation where the actual value sometimes differs from the configured value.

Access Control List Number Sorting Behavior on Phone Number Searches

The following information explains how Oracle® Communications Security Shield Cloud Service (Security Shield) sorts phone numbers when you perform a phone number search on an access control list. Security Shield uses the longest matched pattern, whether from a regular entry or from a wild card entry, to return search results. A regular entry will return an exact match and the wild card entry will return the phone number with the fewest wild card characters.

The scenarios used for the explanation assume that the database contains two tables. One table contains regular phone numbers, which contain no wild card characters, and the other table contains phone numbers that contain wild card characters.

The following table contains the list of regular phone numbers used for the subsequent explanation in this topic.

Table 7-1 Regular Entries

ID	List ID	Phone Number	Action	Direction
1	101	9871562313	Allow	Inbound
3	101	+9871562313	Block	Inbound
5	101	1234567890	Block	Outbound
7	101	3276458901	Allow	Inbound
9	101	774436712	Block	Outbound

The following table contains the list of phone numbers with wild cards used for the subsequent explanation in this topic.

Table 7-2   Wild card Entries

ID	List ID	Phone Number	Action	Direction
2	101	98715623XX	Allow	Inbound
4	101	+9871XXXXXX	Block	Inbound
6	101	1XXXXXXXXX	Block	Outbound
8	101	8373XXXXXX	Allow	Inbound
10	101	77442671X	Allow	Outbound
12	101	12XXXXXXXX	Allow	Outbound
14	101	123XXXXXXX	Block	Outbound
16	101	1234XXXXXX	Allow	Outbound
18	101	12345XXXXX	Block	Outbound
20	101	123456XXXX	Allow	Outbound
22	101	1234567XXX	Block	Outbound
24	101	12345678XX	Allow	Outbound
26	101	123456789X	Block	Outbound
28	101	123456782X	Block	Inbound

Longest Match Scenarios

The following scenarios explain how the Security Shield bases its search results on the longest pattern match.

- Regular Entries—Assume that Security Shield receives a lookup request for 1234567890, which is an Outbound call. Our example database includes ten numbers that match this pattern. The first match is a direct match, which is the regular entry ID 5. Other matches come from the wild card table with IDs 6, 12, 14, 16, 18, 20, 22, 24 and 26, as X can represent any number from 0-9. Because the regular entry 1234567890 is a direct match, Security Shield discards other entries and displays only 1234567890 as the response.
- Wild card Entries—Assume that Security Shield receives a lookup request for 1234567891. The Regular Entries table contains no matching number, but the Wild card Entries table displays potential matches in IDs 6, 12, 14, 16, 18, 20, 22, 24 and 26. Security Shield seeks the longest match among those IDs, which comes from the wild card pattern with the fewest number of wild card characters (X). ID 26 satisfies the criteria and Security Shield displays 123456789x as the response.

Sorting Order Rules

Security Shield bases the sort order on the following rules;

- Security Shield sorts the results by the length of the number. For example, the Regular Entry with ID 9 and the Wild card Entry with ID 10 both have a length equal to nine characters or digits, therefore these phone numbers come before numbers with a length greater than nine characters or digits in ascending order and the opposite in descending order.
- If a number contains the plus character (+) it earns lower priority in the sorting order than the same number that does not containing plus character in ascending

order and high priority in descending order. For example, Regular Entry with ID 1 (9871562313) and with ID 3 (+9871562313), In Ascending order the correct order is 9871562313 > +9871562313 and in descending order it is +9871562313 > 9871562313.

- Wild cards always earn lower priority than regular numbers after some of the digits have been directly matched and opposite for descending order. For example, Regular Number 1234567890 will always come before 123456789X in ascending order and the opposite in descending order.

Descending Order

The following list shows the descending sort order for the results of the preceding example entries.

+9871XXXXXX

98715623XX

+9871562313

9871562313

9871562313

8373XXXXXX

3276458901

1XXXXXXXXX

12XXXXXXXX

123XXXXXXX

1234XXXXXX

12345XXXXX

123456XXXX

1234567XXX

12345678XX

123456789X

1234567890

123456782X

774436712

77442671X

Ascending Order

The following list shows the ascending sort order for the results of the preceding example.

77442671X

774436712

123456782X

1234567890

123456789X

12345678XX

1234567XXX

123456XXXX

12345XXXXX

1234XXXXXX

123XXXXXXX

12XXXXXXXX

1XXXXXXXXX

3276458901

8373XXXXXX

9871562313

+9871562313

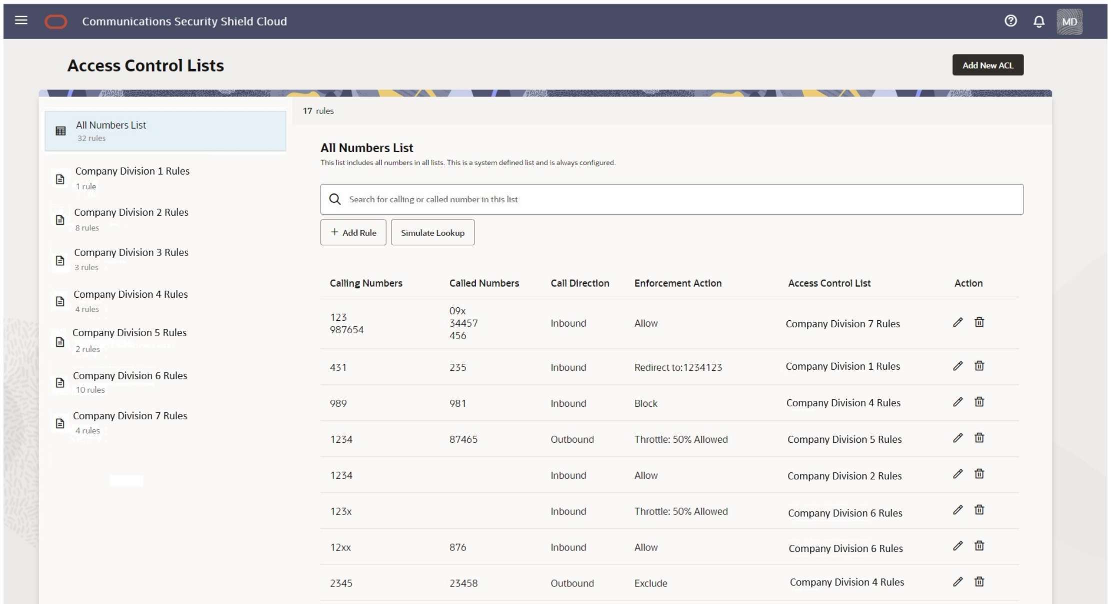
98715623xx

+9871xxxxxx

The All Numbers List

On the Access Control List page, the Oracle® Communications Security Shield Cloud Service (Security Shield) displays the system-named All Numbers List. The All Numbers list is a summary view of all your access control lists. You can edit and delete phone numbers on the All Numbers List and add new numbers. You cannot rename or delete the All Numbers list.

The Access Control List page always displays the All Numbers List as the first list in the left pane. In the right pane, the All Numbers List displays the Search field, the Simulate Lookup button, and the Add Rule button. The display lists the phone numbers and their attributes under the Calling Numbers, Called Numbers, Call Direction, Enforcement Action, Access Control List headings and the Actions icons. The pane also includes a description of the list, when one exists. (You can write a description for any user-created list.) If you do not know which list contains the phone number you want to edit, use Search on the All Numbers List. The search results identify the list.



Access Control Lists

- All Numbers List — 32 rules
- Company Division 1 Rules — 1 rule
- Company Division 2 Rules — 8 rules
- Company Division 3 Rules — 3 rules
- Company Division 4 Rules — 4 rules
- Company Division 5 Rules — 2 rules
- Company Division 6 Rules — 10 rules
- Company Division 7 Rules — 4 rules

17 rules

All Numbers List

This list includes all numbers in all lists. This is a system defined list and is always configured.

Search for calling or called number in this list

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
123 987654	09x 34457 456	Inbound	Allow	Company Division 7 Rules	
431	235	Inbound	Redirect to:1234123	Company Division 1 Rules	
989	981	Inbound	Block	Company Division 4 Rules	
1234	87465	Outbound	Throttle: 50% Allowed	Company Division 5 Rules	
1234		Inbound	Allow	Company Division 2 Rules	
123x		Inbound	Throttle: 50% Allowed	Company Division 6 Rules	
12xx	876	Inbound	Allow	Company Division 6 Rules	
2345	23458	Outbound	Exclude	Company Division 4 Rules	

Note:

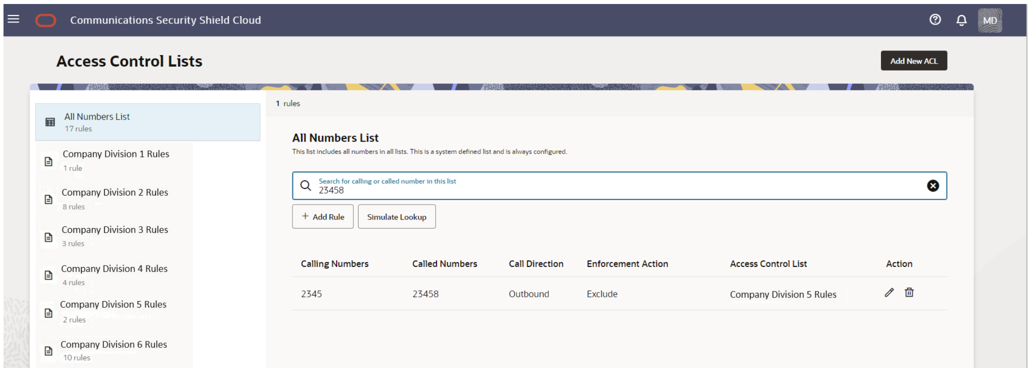
When you add phone numbers, edit phone number attributes, and delete phone numbers on one of your user-created access control lists, the All Numbers List reflects the same information.

Search Field

At the top-left of the right pane, the All Numbers List displays the Search field. Use Search when looking for an exact match to a phone number.

Search supports searching for phone numbers that include wild card characters in the suffix. For example, 1615410x. Any number matching this search criteria from left to right (exact match) is a match. The following are matches: +1615410x, +1615410xx, and +1615410xxx.

You can also perform partial-number search by typing as much of the first part of a phone number as you want and omit the trailing numbers. For example, suppose you want to see all phone numbers that begin with +1 615 410 because you are looking for +1 615 410 0001 or you want to see all numbers with the +1 615 410 prefix. Enter +1 615 410 in Search and the system will display all phone numbers that begin with +1 615 410. For each phone number found on the All Numbers List, the results also show the specified call direction, the specified enforcement action, and the name of the user-created list that contains the phone number, as shown in the following screen capture.



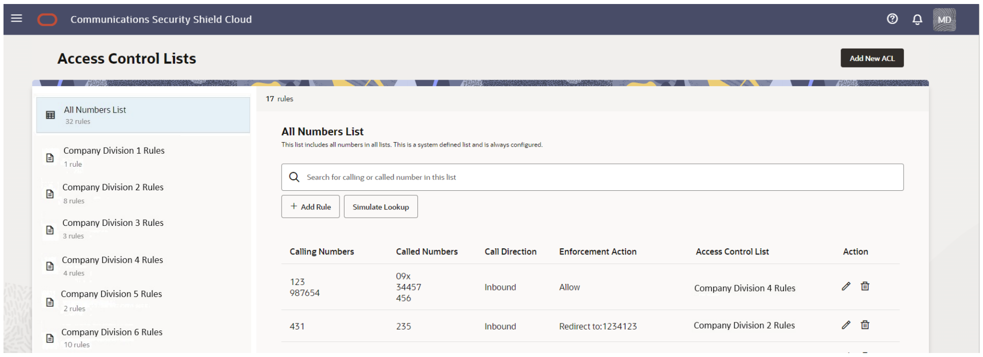
All Numbers List

This list includes all numbers in all lists. This is a system defined list and is always configured.

Search for calling or called number in this list: 23458

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
2345	23458	Outbound	Exclude	Company Division 5 Rules	✎ 🗑

- Match found—The Access Control Lists page displays the Calling Numbers, Called Numbers, Call Direction,Enforcement Action, and name of the list that contains the number, as shown in the following screen capture.

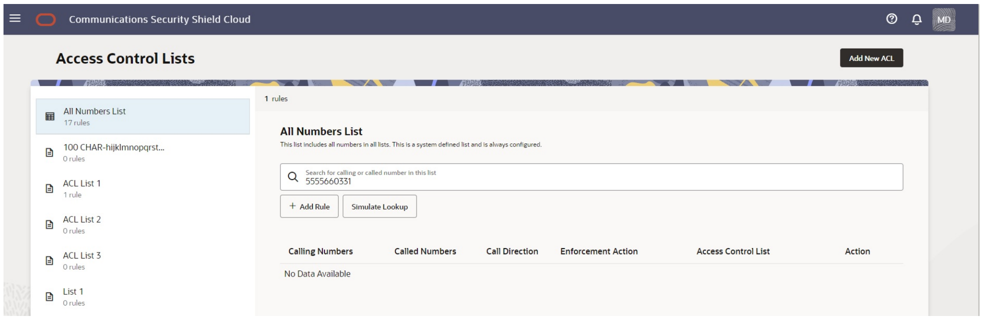


All Numbers List

This list includes all numbers in all lists. This is a system defined list and is always configured.

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
123 987654	09x 34457 456	Inbound	Allow	Company Division 4 Rules	✎ 🗑
431	235	Inbound	Redirect to:1234123	Company Division 2 Rules	✎ 🗑

- No match found—The Access Control Lists page displays a message that says "No Data Available". If you want to add the number to the list, click **+ Add Rule**. When you save the rule, the system adds it to the All Numbers List and to the user-created list that you specified (if you specified one).



All Numbers List

This list includes all numbers in all lists. This is a system defined list and is always configured.

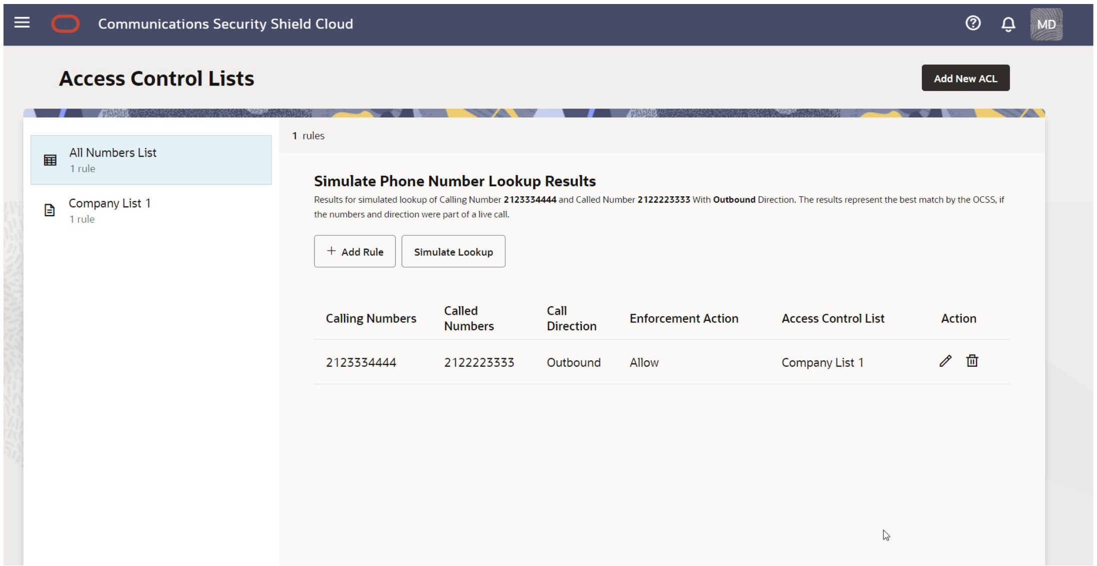
Search for calling or called number in this list: 5555660331

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
No Data Available					

> **Note:**
>
> Search can display up to 1,000 results, which you can scroll through. The results display in ascending order, only

Simulate Lookup Button

Near the top-right of the right pane, the All Numbers List page displays the Simulate Lookup button. Use Simulate Lookup when you want to know how the Security Shield will enforce access control on a phone number on your list. The results show the Call Direction, the Enforcement Action that the session border controller will apply, and the name of the list that contains the phone number, as shown in the following screen capture.



Access Control Lists

All Numbers List
1 rule

Company List 1
1 rule

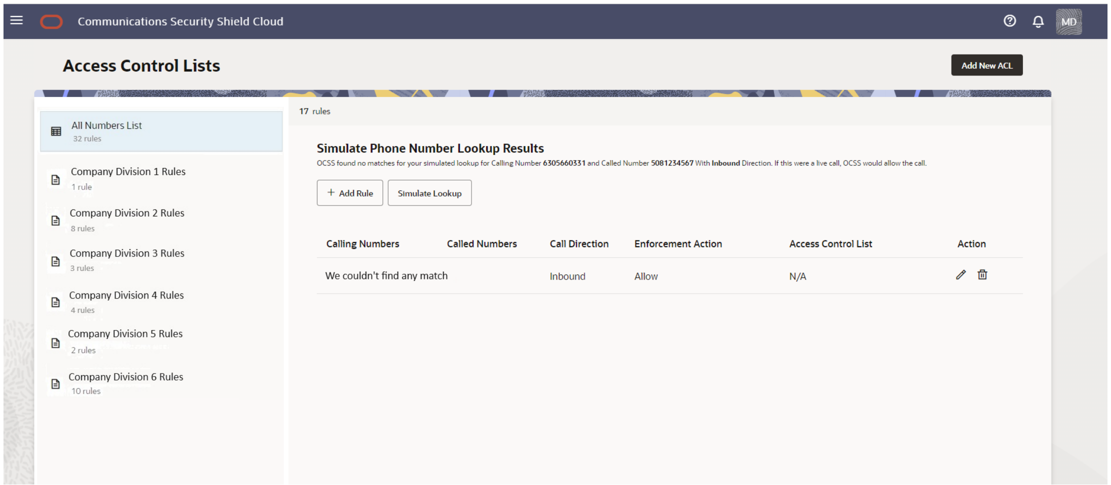
1 rules

Simulate Phone Number Lookup Results

Results for simulated lookup of Calling Number **2123334444** and Called Number **2122223333** With **Outbound** Direction. The results represent the best match by the OCSS, if the numbers and direction were part of a live call.

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
2123334444	2122223333	Outbound	Allow	Company List 1	

When Simulate Lookup does not find a match to the number you entered, the GUI allows the call because the phone number does not exist on any of your access control lists. The Simulate Phone Number Lookup Results page displays the "We couldn't find any match" message as shown in the following screen capture.



Access Control Lists

All Numbers List
32 rules

Company Division 1 Rules
1 rule

Company Division 2 Rules
8 rules

Company Division 3 Rules
3 rules

Company Division 4 Rules
4 rules

Company Division 5 Rules
2 rules

Company Division 6 Rules
10 rules

17 rules

Simulate Phone Number Lookup Results

OCSS found no matches for your simulated lookup for Calling Number **6305660331** and Called Number **5081234567** With **Inbound** Direction. If this were a live call, OCSS would allow the call.

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List	Action
We couldn't find any match		Inbound	Allow	N/A	

Add a New Access Control List

You can create your own access control lists to organize phone numbers and rules for how you want to control inbound and outbound calls. Oracle® Communications Security Shield Cloud Service (Security Shield) supports up to ten user-created access control lists.

Procedure

1. Access the Access Control Lists page.
2. On the Access Control Lists page, click **Add New ACL**.

   Security Shield opens the **Add Access Control List** drawer.
3. In the **Name** field, enter a unique name for the list. 100 characters, maximum.

4. Optional—In the **Description** field, enter a description of the list. 256 characters, maximum.
5. Do one of the following:
   - To add only one list, click **Add**. Security Shield closes the dialog and saves the list.
   - To add another list, click **Add Another**. Security Shield re-displays the Add Access Control List drawer. After you create the last rule you want, click **Add** to close the drawer and save the lists.

Delete an Access Control List

When you want to delete an Oracle® Communications Security Shield Cloud Service (Security Shield) access control list, you can do so at any time from the Access Control List page.

1. Access the **Access Control Lists** page.
2. On the Access Control Lists page, hover over the list that you want to delete, and click the **delete icon**.

   The system displays a confirmation dialog.
3. Click **Delete**.

   Security Shield saves the change.

Edit the Name of an Access Control List

When you want to edit the name of an Oracle® Communications Security Shield Cloud Service (Security Shield) access control list, you can do so at any time from the Access Control List page.

Procedure

1. Access the **Access Control Lists** page.
2. On the Access Control Lists page, hover over the list that you want to edit, and click the **edit icon**.

   Security Shield displays the Edit Access Control List drawer.
3. In the **Name** field, edit the name of the list.
4. Optional—Edit the **Description** field.
5. Click **Save**.

   Security Shield saves the change.

Add a New Rule to an Access Control List

When you want to add one or more rules to an Oracle® Communications Security Shield Cloud Service (Security Shield) access control list, you can do so at any time from the Access Control Lists page.

Procedure
In the following procedure, you can specify one or more Calling Numbers, Called Numbers, or both for the rule to use as criteria for matching calls to the enforcement action. You can select only one call direction per rule.

Phone numbers must be from 1-25 digits or in E.164 international format. You can use the x character as a wild card for number ranges, but only as a suffix. For example, To specify an 11-digit number in the range +1 603-555-0000 to +1 603-555-9999, enter +1 603-555-xxxx.

> **Note:**
>
> If you try to add the same phone number with the same attributes to two access control lists, the system displays an error message.

1. Access the Access Control Lists page.
2. In the left pane, select the list you want to edit.
3. In the right pane, click **+ Add Rule**.
4. In the Add ACL Rule drawer, do the following:
    a. Calling Numbers—Specify one or more Calling Numbers for this rule by entering the number and clicking the + button. You can add up to 100 Calling Numbers per rule.
    b. Called Numbers—Specify one or more Called Numbers for this rule by entering the number and clicking the + button. You can add up to 100 Called Numbers per rule.
    c. Call Directions—Select either Inbound or Outbound for this rule. Default: Inbound. Valid values: Inbound | Outbound.
    d. Enforcement Action—Select an enforcement action for this rule from the drop-down list. Default: Allow. Valid values: Allow | Block | Throttle | Exclude | Redirect (Not supported for Outbound calls).
    e. (Conditional)—If you selected Redirect for the enforcement action, enter a number in the Redirect To Number field. Enter 1-15 digits or a number in E.164 international format. Redirect does not support wild cards or the Outbound call direction.
    f. (Conditional)—If you selected Throttle for the enforcement action, set a number in the Percentage Allowed field. Default: 50%. Valid values: 1%-99%.
5. Do one of the following:
    - To add only one rule, click **Add**. Security Shield closes the drawer and saves the rule.
    - To add another rule, click **Add Another**. Security Shield re-displays the Add ACL Rule drawer. After you enter the last rule you want to create, click **Add** to close the drawer and save the rules.

Delete a Rule from an Access Control List

When you want to delete one or more rules from an Oracle® Communications Security Shield Cloud Service (Security Shield) access control list, you can do so at any time from the Access Control List page.

Procedure

> **Note:**
>
> If you do not know which list contains the rule you want to delete, use Search on the All Rules List. The search results will identify the list.

1. Access the Access Control Lists page.
2. On the All Numbers List page, go to the list that contains the rule you want to delete and click the delete icon.

   Security Shield displays a confirmation dialog.
3. Click **Delete**.

   Security Shield deletes the rule.

Edit a Phone Number on an Access Control List Rule

When you want to edit phone a number in an Oracle® Communications Security Shield Cloud Service (Security Shield) Access Control List, you can do so at any time from the Access Control List page.

Procedure

> **Note:**
>
> If you do not know which list contains the phone number you want to edit, use Search on the All Rules List. The search results identify the list that contains the number.

1. Access the Access Control Lists page.
2. On the Access Control Lists page, locate the list that contains the number you want to edit and click the corresponding edit icon.

   Security Shield opens the Edit ACL Rule drawer.
3. In the Edit ACL Rule drawer, edit any of the fields or parameters that you want to change.

   > **Note:**
   >
   > The rule and call direction must be unique among all your access control lists.
4. Click **Save**.

   Security Shield saves the change.

Change the Call Direction for an Access Control List Rule

When you want to change the call direction on an Oracle® Communications Security Shield Cloud Service (Security Shield) access control list rule, you can do so at any time from the Access Control Lists page.

Procedure

> **Note:**
>
> If you do not know which list contains the rule you want to edit, use Search on the All Rules List. The search results will identify the list that contains the number.

1. Access the Access Control Lists page.
2. On the Access Control Lists page, locate the list that contains the number you want to edit and click the corresponding edit icon.

   Security Shield opens the Edit ACL Rule drawer.
3. In the Edit ACL Rule drawer, go to Call Direction, and change the call direction. Default: Inbound. Valid values: Inbound | Outbound.

   > **Note:**
   >
   > The rule and call direction must be unique among all your access control lists.
4. Click **Save**.

   Security Shield saves the change.

Change the Enforcement Action on an Access Control List Rule

When you want to change the enforcement action on an Oracle® Communications Security Shield Cloud Service (Security Shield) Access Control List Rule, you can do so at any time from the Access Control List page.

Procedure
Because Security Shield allows you to change the enforcement action on a particular rule, be aware that the purpose of the access control list might start to loose meaning or become confusing when you change the enforcement action on a rule.

For example, suppose an access control list is named "Allow Inbound Calls" and you change the enforcement action on a rule in that list to "Block". The block rule still belongs to the "Allow Inbound Calls" list, which can cause confusion because the enforcement action does not correspond to the list name. Oracle recommends either renaming the list or moving the changed number to a list of blocked numbers. If you do not have one, you can create one.

> **Note:**
>
> If you do not know which list contains the rule you want to edit, use Search on the All Rules List. The search results will identify the list that contains the number.

1. Access the Access Control Lists page.
2. On the Access Control Lists page, locate the list that contains the number you want to edit and click the corresponding edit icon.

   Security Shield opens the Edit ACL drawer.

3. In the Edit ACL Rule drawer, go to Enforcement Action and change the action. Default: Allow. Valid values: Allow | Block | Throttle | Exclude | Redirect (Not valid for Outbound calls).
4. Conditional—If you select Redirect, enter the Redirect To Number.
5. Conditional—If you select Throttle, set the Percentage Allowed.
6. Click **Save**.

   Security Shield saves the change.

Simulate a Phone Number Lookup

When you want to know what enforcement action your Session Border Controller will apply to a phone number, or which of your Oracle® Communications Security Shield Cloud Service (Security Shield) Access Control lists contains a phone number, use the Simulate Lookup function.

Procedure
In the following procedure, you must enter both the Called Number and the Calling Number. Simulate Lookup cannot return a result with only one or the other. Simulate Phone Number Lookup does not accept wild cards.

1. Access the Access Control Lists page and select the All Rules List.
2. On the All Numbers List, click **Simulate Lookup**.
3. In the Simulate Phone Number Lookup dialog, do the following:
   - Calling Number—Enter the complete Calling Number.
   - Called Number—Enter the complete Called Number.
   - Call Direction—Set the call direction. Default: Inbound. Valid values: Inbound | Outbound.
4. Click **Lookup**.

   Security Shield displays the result, which includes the Enforcement Action and name of the Access Control List that contains the phone number.

8

Outbound Number Management

Oracle® Communications Security Shield Cloud Service (Security Shield) Outbound Number Management provides tools to help you manage outbound calls for your enterprise. You can create a list of outbound phone numbers and specify how Security Shield validates and enforces their use.

Use the following topics to create and manage your enterprise outbound calling number lists.

Topics:

- Fraud and Spam Mitigation Details
- Trusted Enterprise Calls
- Outbound Call Processing Behavior
- Outbound Number Management Controls and Actions
- Outbound Numbers Management - Outbound Numbers Tab
- Outbound Number Management - Settings Tab

Fraud and Spam Mitigation Details

Oracle® Communications Security Shield Cloud Service (Security Shield) fraud and spam mitigation allows you to specify which of your telephone numbers your call recipients see. In this way, you can enforce the use of general numbers for outbound calls to replace the telephone numbers directly associated with an employee, agent, or associate.

Fraud and spam mitigation can also help you ensure that your outbound calls use the correct number format. Short numbers, for example from an internal dialing plan, can lead to blocked calls and lower answer rates. In addition, using the correct number format also supports call attestation performed by SIP trunk providers and other carriers (also known as STIR/SHAKEN) to combat Robocalls.

Use the following topics to create and manage your enterprise outbound calling number lists.

- Outbound Call Processing Behavior
- Outbound Number Management Controls and Actions
- Outbound Numbers Management - Outbound Numbers Tab
- Outbound Number Management - Settings Tab

Trusted Enterprise Calls

In addition to the fraud and spam protection that Oracle® Communications Security Shield Cloud Service (Security Shield) provides, the Trusted Enterprise Calls service supports specifying which of your telephone numbers you want digitally signed using STIR/SHAKEN Authentication.

For more information, see:

- Security Shield Subscriptions
- Security Shield Features per Subscription

Outbound Call Processing Behavior

To help manage your enterprise phone numbers allowed for outbound calls, you can create a list of allowed outbound phone numbers for Oracle® Communications Security Shield Cloud Service (Security Shield).

With Outbound Number Management, you can configure attributes and rules for phone numbers on the list to instruct how you want Security Shield to handle your outgoing calls.

- When Security Shield finds a match on the list for an outbound calling number it handles the call according to the rules you set.
- When Security Shield cannot find a match on the list for an outbound calling number it allows the call and sends the outbound INVITE with no changes, by default. When left in the default state, Security Shield cannot detect calls from numbers with a "Do Not Originate" policy, illegitimate numbers, or numbers that do not exist in your set of telephone numbers. You can change the behavior by setting the call treatment to block calls from phone numbers not on the list. Even when no match is found, and the respective setting is to allow the call, Security Shield can still block the outbound call because of the Access Control List. Outbound calls are also subject to reputation score and Toll Fraud either of which can influence the call treatment.
- When you configure a presentation number for an outbound calling number, Security Shield replaces the original number in the FROM header of the outbound INVITE with the presentation number configured for the calling number. You can use the presentation number to ensure your outgoing calls present, for example, only the main company number, main toll-free number (for your contact center), switchboard number, and so on. This can help to shield your employees from a direct dial-in or callback.
- When the calling number is on the list and you set the status for the number to Inactive, Security Shield handles the call based on the settings for Inactive (on the Settings tab).
- When the original number is in the sip-uri format and you want Security Shield to use a presentation number, the Security Shield adds the presentation number in sip-uri format and preserves any header parameters or parameters as received.
- When the original FROM contains Anonymous in the display name or elsewhere, Security Shield overrules it in the replaced FROM.
- When the number is present in your enterprise number table, is marked active, and is marked to use PAI, Security Shield behaves as follows:
  - removes any preexisting headers, including anonymous information.
  - removes a received P-Preferred Identity (PPI)
  - does not take into account privacy headers related to the FROM and keeps the privacy header in the outbound INVITE.
  - adds a new PAI header to the outbound call.
  - populates the new PAI header with the presentation number when you provision PAI for the calling number or populates the PAI header with the

original calling number when you do not configure a presentation number for the calling number.

- if the original FROM is in tel-uri format, adds PAI in tel-uri format.
- if the original FROM is in sip-uri, adds the PAI in sip-uri format where user name consists of presentation number, re-use the host name as received in the FROM and add tag user=phone.
- if anonymous is present in the host name of the original FROM, uses the provisioned domain name.

- For outbound calls, any Header Manipulation Rules that change the domain part of the FROM header will overwrite the domain name provided by Security Shield.

Outbound Number Management Controls and Actions

The Oracle® Communications Security Shield Cloud Service (Security Shield) Outbound Number Management page displays actions and controls for creating lists of outbound phone numbers and configuring how you want to control their use.

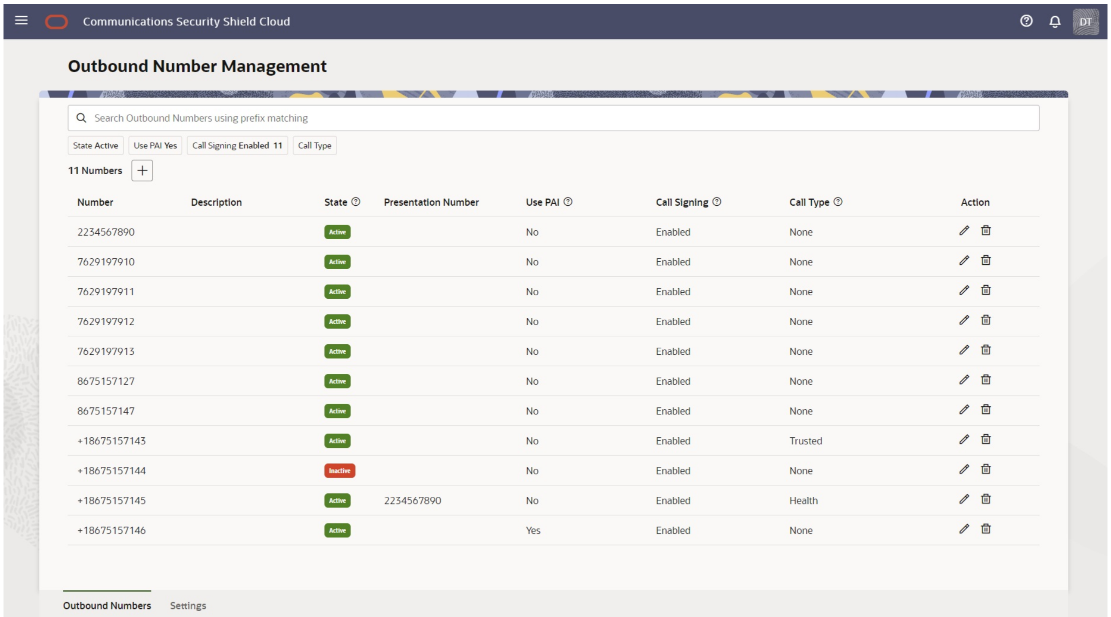
Outbound Numbers Tab

The Outbound Number Management page displays the Outbound Numbers tab by default. Use the Outbound Numbers tab to see information about existing numbers, add numbers, and search for numbers. The tab includes the search field, filter chips to refine a search, and the add numbers button. See Outbound Number Attributes for descriptions of the columns.

The Security Shield Outbound Numbers tab is where you create your outbound calling numbers list and later search for a phone number, for example, to edit its attributes or to delete the number.

Note:

The Call Signing column displays only for Trusted Enterprise Call subscribers.



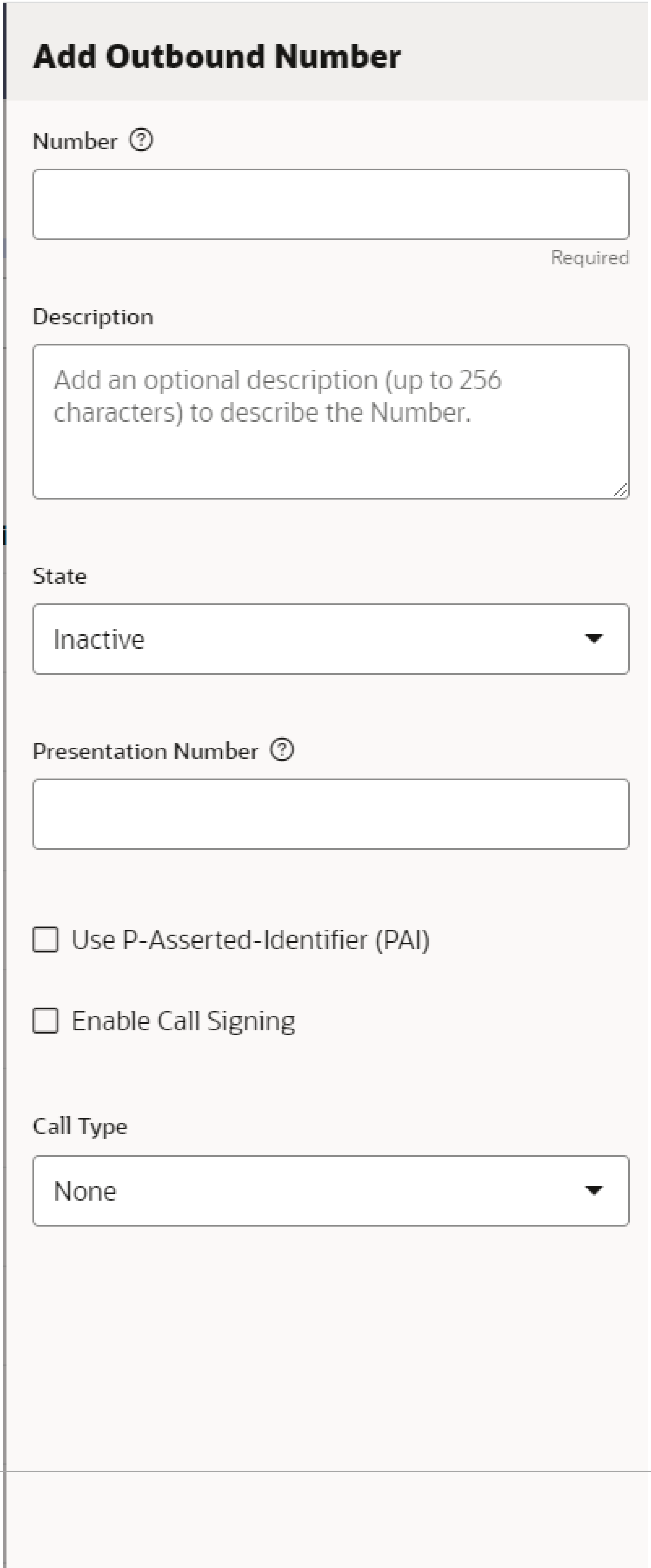
Outbound Number Management

Search Outbound Numbers using prefix matching

11 Numbers +

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Action
2234567890		Active		No	Enabled	None	
7629197910		Active		No	Enabled	None	
7629197911		Active		No	Enabled	None	
7629197912		Active		No	Enabled	None	
7629197913		Active		No	Enabled	None	
8675157127		Active		No	Enabled	None	
8675157147		Active		No	Enabled	None	
+18675157143		Active		No	Enabled	Trusted	
+18675157144		Inactive		No	Enabled	None	
+18675157145		Active	2234567890	No	Enabled	Health	
+18675157146		Active		Yes	Enabled	None	

To add numbers to the list, click the Add button to display the Add Outbound Calling Number drawer, where you add phone numbers one at a time and specify their attributes. The only required field is the Number field. You can set any combination of the attributes or none at all. When you set no attributes, the phone number defaults to the Inactive state.



Add Outbound Number

Number ⓘ

Required

Description

Add an optional description (up to 256 characters) to describe the Number.

State

Inactive

Presentation Number ⓘ

☐ Use P-Asserted-Identifier (PAI)

☐ Enable Call Signing

Call Type

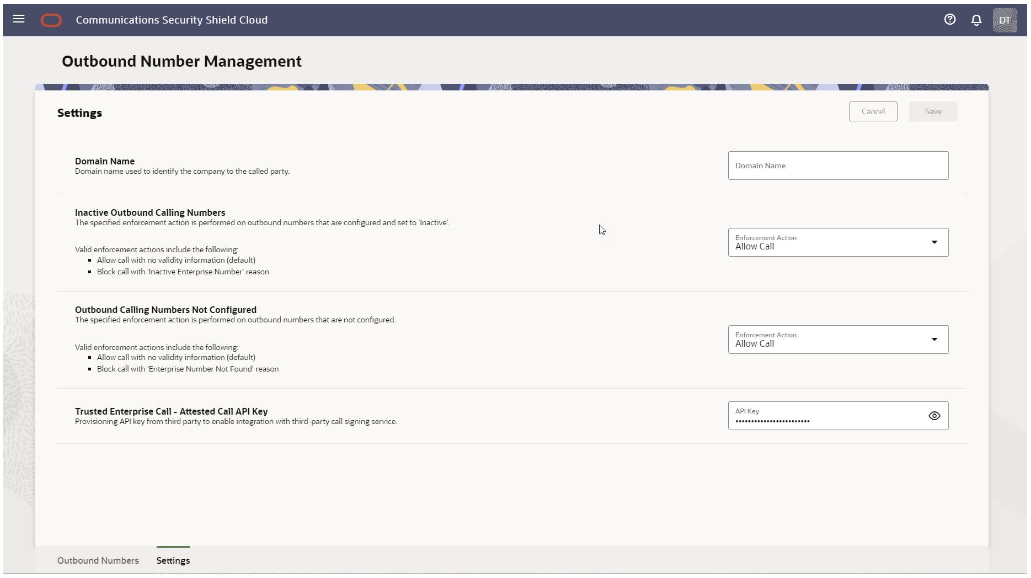
None

See Outbound Number Attributes and Call Type Descriptions.

Settings Tab

Use the Settings tab to configure how you want Security Shield to handle outbound calls.

> **Note:**
>
> The Trusted Enterprise Call - Attested Call API Key attribute displays only for Trusted Enterprise Call - Bring Your Own License subscribers.



Outbound Number Management

Settings

Domain Name
Domain name used to identify the company to the called party.

Domain Name

Inactive Outbound Calling Numbers
The specified enforcement action is performed on outbound numbers that are configured and set to 'Inactive'.

Valid enforcement actions include the following:
- Allow call with no validity information (default)
- Block call with 'Inactive Enterprise Number' reason

Enforcement Action: Allow Call

Outbound Calling Numbers Not Configured
The specified enforcement action is performed on outbound numbers that are not configured.

Valid enforcement actions include the following:
- Allow call with no validity information (default)
- Block call with 'Enterprise Number Not Found' reason

Enforcement Action: Allow Call

Trusted Enterprise Call - Attested Call API Key
Provisioning API key from third party to enable integration with third-party call signing service.

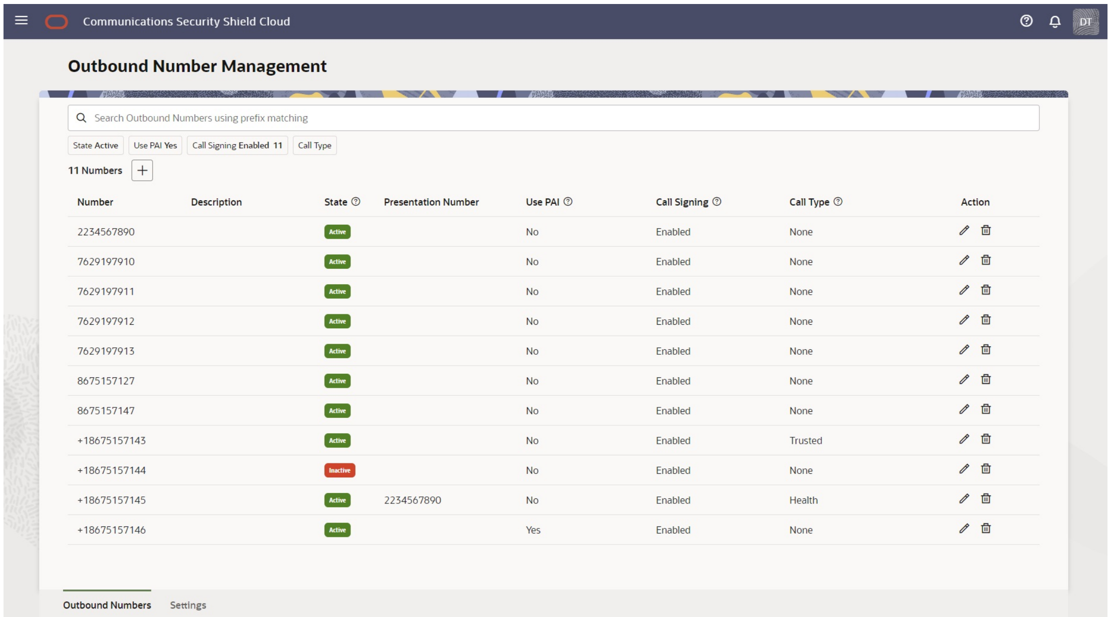
API Key: ••••••••••••••••••••••••

Outbound Numbers Management - Outbound Numbers Tab

The Oracle® Communications Security Shield Cloud Service (Security Shield) Outbound Numbers tab is where you create your outbound calling numbers list and later search for a phone number, for example, to edit its attributes or to delete the number.

The following screen capture shows the Outbound Numbers tab with sample data.

> **Note:**
>
> The Call Signing column displays only for Trusted Enterprise Call subscribers.


Communications Security Shield Cloud
DT
Outbound Number Management
Search Outbound Numbers using prefix matching
State Active
Use PAI Yes
Call Signing Enabled 11
Call Type
11 Numbers
+
Outbound Numbers
Settings

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Action
2234567890		Active		No	Enabled	None	
7629197910		Active		No	Enabled	None	
7629197911		Active		No	Enabled	None	
7629197912		Active		No	Enabled	None	
7629197913		Active		No	Enabled	None	
8675157127		Active		No	Enabled	None	
8675157147		Active		No	Enabled	None	
+18675157143		Active		No	Enabled	Trusted	
+18675157144		Inactive		No	Enabled	None	
+18675157145		Active	2234567890	No	Enabled	Health	
+18675157146		Active		Yes	Enabled	None	

Use the Search field to find phone numbers on the list. See Search Operations on the Outbound Numbers List .

Click the "plus" character button to display the Add Outbound Calling Number drawer, where you add phone numbers one at a time and specify their attributes. See Add a New Phone Number to the Outbound Number Management List.

Outbound Number Attributes

In the Oracle® Communications Security Shield Cloud Service (Security Shield) Add Outbound Number drawer you can set the attributes that you want applied to an outbound calling phone number. Security Shield requires only the phone number. You can configure some, all, or none of the attributes. Reach the drawer from the Outbound Call Management tab.

The outbound call attributes you can set for a phone number include:

- Number—The general number format convention is country code followed by the subscriber phone number <country code><subscriber phone number>. The country code can be up to three digits long. The subscriber phone number may include an area code and is typically seven to eleven digits long, depending on the national number conventions. For international formatting, you may format the number with a + character (+<country code><subscriber phone number>, for example, +15551234567) or without the + character. For outbound calls to international destinations you can use either the + character or the international dialing prefix for your country. Using the format as described helps to achieve the goal of call spam labeling and helps to elevate STIR-SHAKEN validation by Communications Service Providers.
- Description (Optional)—A descriptive name for the number. For example, Enterprise Callback Number.
- State (Optional)—Determines whether the rule applies to the number at a given moment. Default: Inactive.
  - Active—The rule you created for the number is executed for calls originating from the specified number. For example, adding P-Asserted Identity and using the Presentation Number either individually or together.

  - Inactive—The number remains on the list and Security Shield allows outbound calls from the number without executing the rules you created.

- Presentation number (Optional)—The phone number you want the call recipient to see. When configuring the Presentation Number use the number format described above in the Number parameter. Depending on the SIP trunk providers you use, you may use the Country Code. For example, in the United States you use [country code][area code][local phone number] or the more commonly used [area code][local phone number]. In the European Union and United Kingdom you use [+][country code][area code][local phone number].
- Use P-Asserted Identity header (PAI) (Optional)—Use to include the PAI header in the outbound call, so the SIP Trunk provider's spam solution analytics, and potentially the nuisance (robocall) analytics applications on smart phones, considers the call from a legitimate source. Using the PAI helps to achieve the goal of call spam labeling and helps to elevate STIR-SHAKEN validation by Communications Service Providers. Default: Deselected.
- Call Signing (Optional)—Displays the enablement state for call signing. Requires the Trusted Enterprise Calls subscription. Default: Enabled. Valid values: Disabled | Enabled.
- Call Type (Optional)—Select a label for the call. Default: None. Valid Values: Business | Debt Collection | Health | Informational | None | Survey | Telemarketing | Trusted.
- Action—Click the pencil icon to edit a number. Click the trash can icon to delete a number.

> **Note:**
>
> You must be a member of the OCSS ACL Editor, OCSS Configuration Editor, or CGBU OCSS Administrator user groups to work with the Outbound Number list. See "User Roles and Privileges" in the *Security Shield Installation and Maintenance Guide*.

Call Type Descriptions

The Oracle® Communications Security Shield Cloud Service (Security Shield) Outbound Number Management page supports the following call types that you can use to filter phone numbers.

- Business—Calls placed by businesses, entities, or enterprises. Use when none of the other call tags apply and you want to add Call Tags to the outbound call.
- Debt Collection—Calls related to collecting of debt, for example, loans, mortgages, and credit.
- Health—Calls to provide health care-related information, for example, from health plans, health care clearinghouses, health care providers, prescriptions, and doctor calls.
- Survey—Calls call that solicit opinions or data from the called party.
- None—Omits call types from the search.
- Informational—Calls intended to communicate information to the called party. For example, an order confirmation, an appointment reminder, or a notice from a utility.

- Telemarketing—Calls placed to sell the call recipient a product or service, or donate to an organization.
- Trusted—Calls from a trusted entity not covered by the other call types. For example, returned calls and messages from telecommunication carriers and utilities. An established business relationship must exist between the caller and the recipient.

> **Note:**
>
> Configuring call types with a value other than the default does not impact the outbound call INVITE.

The Call Type list on the Outbound Number Management tab shows all call types for configuration purposes. When you filter on call types, the filter menu displays only the call types you configured.

See Add a New Phone Number to the Outbound Number Management List

Outbound Call Signing

Oracle® Communications Security Shield Cloud Service (Security Shield) outbound call signing informs the terminating mobile service provider that the call originated from a legitimate source; you. Outbound call signing uses a cryptographic signature and JSON Web Token so the terminating mobile service provider can verify the call details to determine its origin.

For customers with the Trusted Enterprise Calls subscription, the Outbound Numbers table displays the Call Signing column and filter chip on the Outbound Numbers tab on the Outbound Number Management page. The tab lists your configured outbound numbers and whether or not they are enabled for outbound call signing, along with other information about each number.

To enable outbound call signing, select a phone number on the Outbound Numbers list to edit or add a new one. Security Shield displays the configuration drawer where you enable outbound call signing per phone number.

> **Note:**
>
> Security Shield logs enabling and disabling outbound call signing. On the Activity Log page, hover over the Timestamp to see the activity details.

- **Customers who purchase call attestation from Oracle**—Enter the phone number, select the Active state, optionally enter a presentation number, and select Enable Call Signing.
- **Customers who want to use their own call signing and attestation vendor or solution**—Enter the phone number, select the Active state, optionally enter a presentation number, select Enable Call Signing, and enter your Neustar API key (on the Settings tab).

> **Note:**
>
> When you enter a presentation number, Security Shield uses that number for outbound call signing and attestation. See Security Shield Phone Number Format Requirements for special presentation number requirements for outbound call signing.

When searching for an existing phone number when the list is long, use the Call Signing filter chip to find phone numbers with Call Signing enabled or disabled.

Search Operations on the Outbound Numbers List

After you create a list of outbound calling numbers for Oracle® Communications Security Shield Cloud Service (Security Shield), you might need to edit the list or search for phone numbers for other reasons. For example, you might want to change the settings for one or more of the attributes or delete a number.

> **Note:**
>
> You must be a member of the OCSS ACL Editor, OCSS Configuration Editor, or CGBU OCSS Administrator user groups to edit or delete numbers in Outbound Numbers Management.

You can search in the following ways:

Search by Phone Number

Use the following guidelines to search for a number.

- The general number format convention is country code followed by the subscriber phone number <country code><subscriber phone number>. The country code can be up to three digits long. The subscriber phone number may include an area code and is typically seven to eleven digits long, depending on the national number conventions. For international formatting, you may format the number with a + character (+<country code><subscriber phone number>, for example, +15551234567) or without the + character. For outbound calls to international destinations you can use either the + character or the international dialing prefix for your country. Check with your SIP trunk provider for the number format convention it supports.
- Enter numbers using a wild card suffix. For example: +1919555xxxx.

Search With Filter Chips

Security Shield provides a set of filter chips (located below the Search field), which are based on the column headers. To refine your search, click one or more filter chips to move them into the Search field. After you put a filter chip into the Search field you can further refine your search by clicking the filter chip to see a list of additional filters. You can add multiple filter chips to Search. You can remove filter chips from the search bar when you no longer want the filter applied, but you cannot delete them from Security Shield. The filter chips provide the following filters.

- **State**—Default: Active. Filter Choices: Active | Inactive.

- **Use PAI**—Default: Yes. Filter Choices: Yes | No.
- **Call Signing Enabled**—(Displays only with the Trusted Enterprise Calls subscription.) Default: Enabled. Filter Choices: Enabled | Disabled.
- **Call Type**—Default: None. Filter Choices: Business | Debt Collection | Health | Informational | None | Survey | Telemarketing | Trusted.

Add a New Phone Number to the Outbound Number Management List

Use the following procedure to add one or more phone numbers the Oracle® Communications Security Shield Cloud Service (Security Shield) outbound number management list.

Before You Begin

- If your Session Border Controller does not use phone numbers in the E.164 format, you may need to work with Oracle before deploying Security Shield to determine how to normalize your phone numbers to work effectively with Security Shield.
- You must be a member of the OCSS ACL Editor, OCSS Configuration Editor, or CGBU OCSS Administrator user groups to add numbers to the Outbound Numbers list. Only the CGBU OCSS Administrator can add, modify, or remove the API key.
- See Security Shield Phone Number Format Requirements.

Procedure
Use the following procedure to add a phone number to the outbound number list. When you enable a phone number for Outbound Call Signing, allow about fifteen days for the service to take effect.

> **Note:**
>
> Customers who use their own call signing and attestation vendor or solution must provision and manage the account, users, phone numbers, and API keys on your vendor's portal.

1. Access the **Outbound Number Management** page and click the **Add** icon.
2. In the **Add Outbound Number** drawer, do the following:
   - Number—Enter the phone number you want to add. Enter 1-15 digits in E.164 international format. You can use the x character as a wild card representing any single digit. The field supports wild cards only for the suffix.
   - Description—(Optional) Enter a description about the purpose of the number. 256 character maximum.
   - State—Select Active when you want Security Shield to execute the rule for the outbound number. Select Inactive to use the Inactive Outbound Numbers enforcement action configured under the Settings tab. Default: Active. Valid values: Active | Inactive.
   - Presentation number—(Optional) Enter the number you want the call recipient to see in caller ID, if different from the calling number. Enter 1-15 digits in E.164 international format. Do not use wild cards.

> **Note:**
>
> Ensure that each of your SIP Trunk providers can use the format you use.

- Use P-Asserted Identifier (PAI) (Optional)—Select to include the PAI header in the outbound call., so Security Shield analytics considers the call legitimate. Default: Deselected.
- Enable Call Signing—(Requires the Trusted Enterprise Call subscription) Select to enable call signing for this phone number.
- Call Type (Optional)—Select a call type from the drop-down list. Default: None. Valid values: Business | Debt Collection | Health | Informational | None | Survey | Telemarketing | Trusted.

3. Do one of the following:
    - Click **Add** to close the drawer and add the phone number to the list.
    - Click **Add Another** to keep the drawer open to add another phone number to the list.

Next Steps

- Customers who use their own call signing and attestation vendor or solution: Go to the Settings tab on the Outbound Number Management page, and enter your Attested Call API Key.

Edit Phone Number Attributes on the Outbound Number Management List

Use the following procedure to edit phone numbers on the Oracle® Communications Security Shield Cloud Service (Security Shield) outbound number management list.

Before You Begin

- If your Session Border Controller does not use phone numbers in the E.164 format, Oracle or a partner may need to work with you before deploying Security Shield to determine how to normalize your phone numbers to work effectively with Security Shield.
- You must be a member of the OCSS ACL Editor, OCSS Configuration Editor, or CGBU OCSS Administrator user groups to add numbers to the Outbound Number list. Only the CGBU OCSS Administrator can add, modify, or remove the API key.
- See Security Shield Phone Number Format Requirements.

Procedure
Use the following procedure to edit phone numbers on the outbound numbers list.

1. Access the **Outbound Call Management** page.
2. On the **Outbound Numbers** tab, use **Search** to find the phone number you want to edit.
3. In the row of the phone number you want to edit, click the **Edit** icon.

    Security Shield displays the Edit Outbound Number Attributes drawer.
4. In the **Edit Outbound Number Attributes** drawer, do the following:

- Number—You cannot edit the phone number, only its attributes. To change the phone number, delete the existing record and add the one you want.
- Description—Edit the description about the purpose of the number.
- State—Select Active when you want Security Shield to execute the rule. Select Inactive when you want Security Shield to use the Inactive Outbound Number enforcement action configured on the Settings tab.
- Presentation number—Edit the number you want the call recipient to see in caller ID. Enter 1-15 digits in E.164 international format. Do not use wild cards.

> **Note:**
>
> Ensure that each of your SIP Trunk providers can use the format you use.

- Use P-Asserted Identifier (PAI)—Select or deselect to include or exclude the PAI header in the outbound call.
- Enable Call Signing —(Requires the Trusted Enterprise Call subscription) Select or deselect to enable or disable call signing for this phone number.
- Call Type—Select a different call type from the list. Valid values: Business | Debt Collection | Health | Informational | None | Survey | Telemarketing | Trusted.

5. Click **Save**.

Delete a Phone Number From the Outbound Number Management List

The simple method for deleting a phone number from the Outbound Number Management list is to enter the number in the Search field and click the delete icon when Oracle® Communications Security Shield Cloud Service (Security Shield) finds the number.

Before You Begin

- You must be a member of the OCSS ACL Editor, OCSS Configuration Editor, or CGBU OCSS Administrator user groups to delete numbers from Outbound Numbers Management.

Procedure
Use the following procedure to delete a phone number without using the Search filters.

1. Access the **Outbound Number Management** page.
2. On the **Outbound Numbers** tab, use **Search** to find the phone number you want to delete.
3. In the row of the phone number you want to delete, click the **Delete** icon.

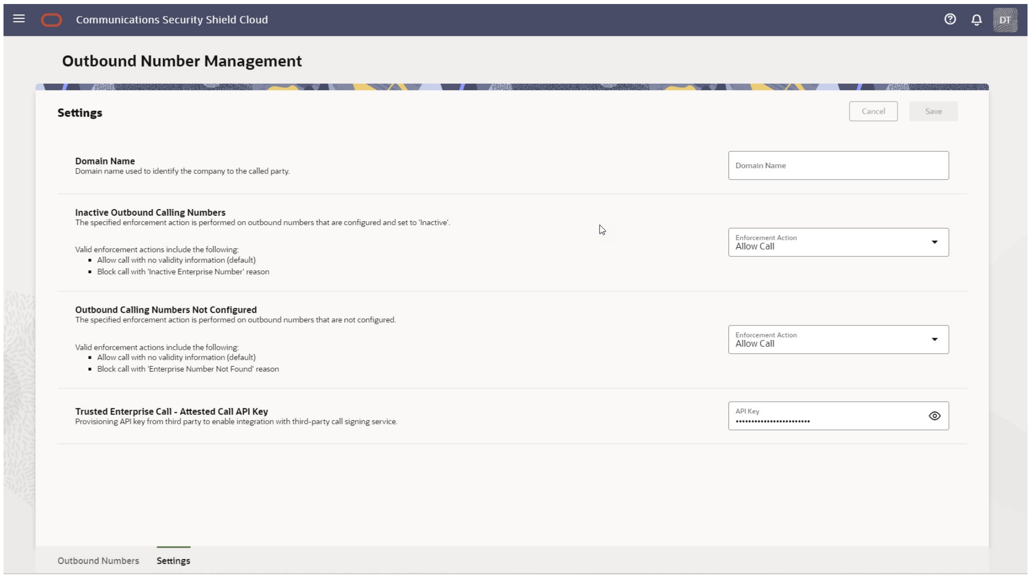
   Security Shield displays a confirmation dialog.
4. Click **Delete**.

Outbound Number Management - Settings Tab

On the Oracle® Communications Security Shield Cloud Service (Security Shield) Outbound Number Management page, click the Settings tab to view and edit your current settings for outbound numbers.

The following screen capture shows the Settings tab, where you set the domain name, enforcement actions for outbound numbers, depending on your subscription, set the API Key for Trusted Enterprise Calls.

> **Note:**
>
> The Trusted Enterprise Call - Attested Call API Key attribute displays only for Trusted Enterprise Call - Bring Your Own License subscribers.



Outbound Number Management

Settings

Domain Name
Domain name used to identify the company to the called party.

Domain Name

Inactive Outbound Calling Numbers
The specified enforcement action is performed on outbound numbers that are configured and set to 'Inactive'.

Valid enforcement actions include the following:
- Allow call with no validity information (default)
- Block call with 'Inactive Enterprise Number' reason

Enforcement Action: Allow Call

Outbound Calling Numbers Not Configured
The specified enforcement action is performed on outbound numbers that are not configured.

Valid enforcement actions include the following:
- Allow call with no validity information (default)
- Block call with 'Enterprise Number Not Found' reason

Enforcement Action: Allow Call

Trusted Enterprise Call - Attested Call API Key
Provisioning API key from third party to enable integration with third-party call signing service.

API Key: ••••••••••••••••••••••••

See Configure Outbound Number Management Settings

Configure Outbound Number Management Settings

Use the Settings tab on the Outbound Number Management page to configure how Oracle® Communications Security Shield Cloud Service (Security Shield) displays your domain name to outbound call recipients, enforces inactive outbound calling numbers, and enforces numbers not configured for Outbound Number Management.

Procedure
Use the following procedure to set or edit outbound number settings.

> **Note:**
>
> The Trusted Enterprise Call - Attested Call API Key attribute displays only for customers who have the Trusted Enterprise Calls Bring Your Own License subscription.

1. Access the **Outbound Number Management** page, and click the **Settings** tab.
2. On the **Settings** tab, do the following:
   - Domain Name—Set the domain name you want the called party to see to identify your company. 100 maximum characters.

> **Note:**
>
> For outbound calls, any Header Manipulation Rules that change the domain part of the FROM header may overwrite the domain name provided by Security Shield.

- Inactive Outbound Calling Numbers—Set the enforcement action you want the session border controller to perform on inactive phone numbers configured for Outbound Number Management. Default: Allow Call. Valid values: Allow Call | Block
- Outbound Calling Numbers Not Configured—Set the enforcement action you want the session border controller to perform on phone numbers not configured in Outbound Number Management. Default: Allow Call. Valid values: Allow Call | Block
- Trusted Enterprise Call - Attested Call API Key—Enter your Neustar API Key, if you have the Security Shield Trusted Enterprise Call - Bring Your Own License subscription. 255 maximum characters.

3. Click **Save**.

9 Number Lookup

Oracle® Communications Security Shield Cloud Service (Security Shield) Number Lookup provides a way to search for a phone number across all of your Security Shield phone number lists. The resulting display shows every list and states whether or not the number is on the list. When Security Shield finds a number on a list, the search results show the settings for the number per type of list. You cannot add numbers to a list or configure any settings from the Number Lookup page. You must go to the page for the list type to do so.

Topics:

Number Lookup Controls and Actions

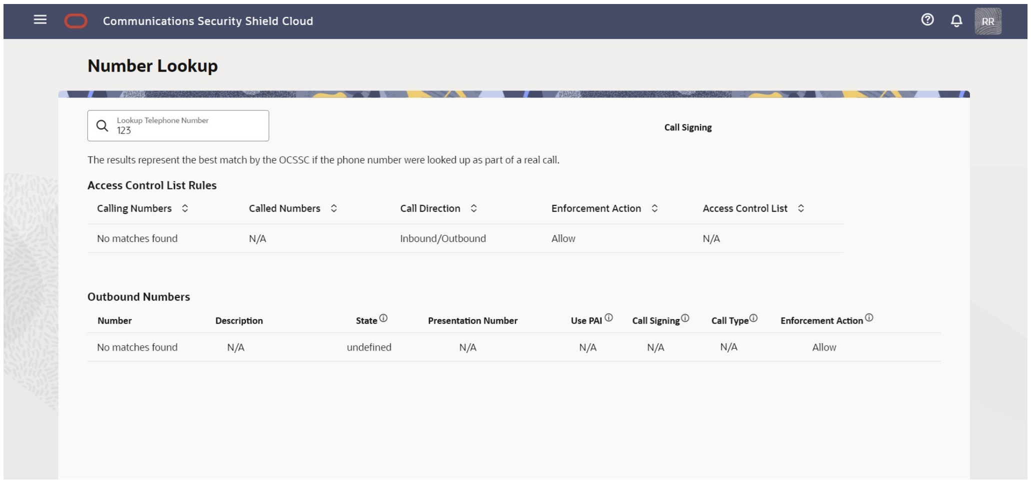
Through the Oracle® Communications Security Shield Cloud Service (Security Shield) Number Lookup page, you can search for a phone number across all of your Security Shield lists. When reporting the results of a search, the Number Lookup page displays a table of lists and shows either "No Match Found" or the phone number and its settings for each list type.

The following scenarios provide some examples of the way the Number Lookup page displays the results of a phone number lookup.

Phone Number In Neither the Access Control List Rules Nor the Outbound Numbers List

When you lookup a phone number that is in neither the Access Control List nor the Outbound Numbers list, the results show "No matches found" and displays the following information:

- Access Control List Rules—The Enforcement action for the searched number is to Allow calls that do not match a number in the list, which is the system default behavior.
- Outbound Numbers—The Enforcement action is Allow because that is the action the user set for "Outbound Calling Numbers Not Configured" in the General Settings configuration for Outbound Number Management page. If, for example, you change Block to Allow for such calls, this display will show Allow as the Enforcement action.



Number Lookup

Lookup Telephone Number
123

Call Signing

The results represent the best match by the OCSSC if the phone number were looked up as part of a real call.

Access Control List Rules

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List
No matches found	N/A	Inbound/Outbound	Allow	N/A

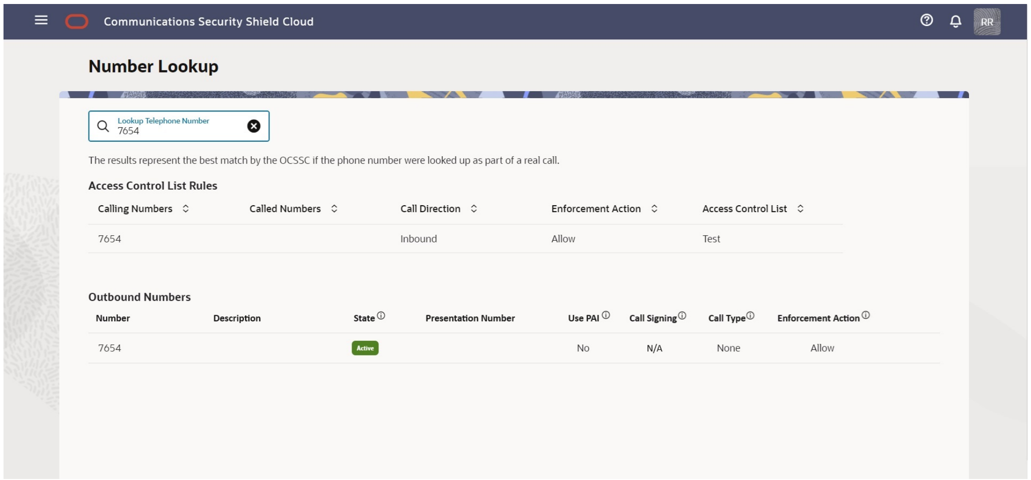
Outbound Numbers

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Enforcement Action
No matches found	N/A	undefined	N/A	N/A	N/A	N/A	Allow

Phone Number Configured on Both the Access Control List Rules and the Outbound Numbers List

When you lookup a phone number that is included in both the Access Control List and the Outbound Numbers list, the results show the phone number in both lists and display the following information:

- Access Control List Rules—The phone number may appear twice when you set configurations for both Outbound and Inbound calls for the number. The results also show the configured enforcement action and the name of the Access Control List that includes the number. In this scenario, two Access Control List Rules include the number.
- Outbound Numbers—The number appears once along with the parameters the user configured on the Outbound Numbers page.



Number Lookup

Lookup Telephone Number
7654

The results represent the best match by the OCSSC if the phone number were looked up as part of a real call.

Access Control List Rules

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List
7654		Inbound	Allow	Test

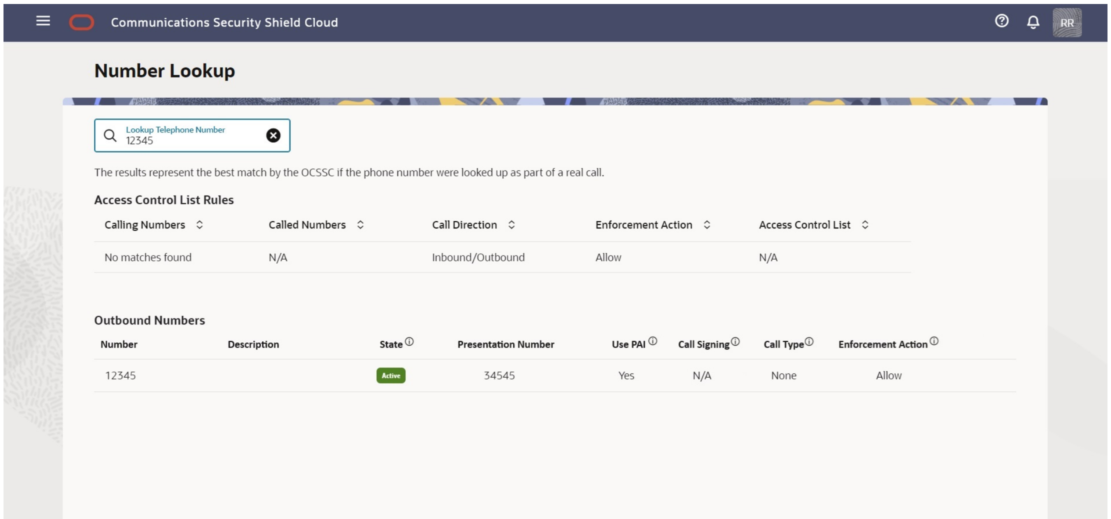
Outbound Numbers

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Enforcement Action
7654		Active		No	N/A	None	Allow

Phone Number Not Configured in the Access Control List Rules and is Configured in the Outbound Numbers

When you look up a number that is not configured in the Access Control List and is included in the Outbound Numbers list, the results show the phone number only in the Outbound Numbers list and displays the following information.

- Access Control List Rules—The Enforcement action for the searched number is to Allow calls that do not match a number in the list, which is the system default behavior.
- Outbound Numbers—The number displays along with the parameters you configured on the Outbound Numbers page.



Number Lookup

Lookup Telephone Number
12345

The results represent the best match by the OCSSC if the phone number were looked up as part of a real call.

Access Control List Rules

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List
No matches found	N/A	Inbound/Outbound	Allow	N/A

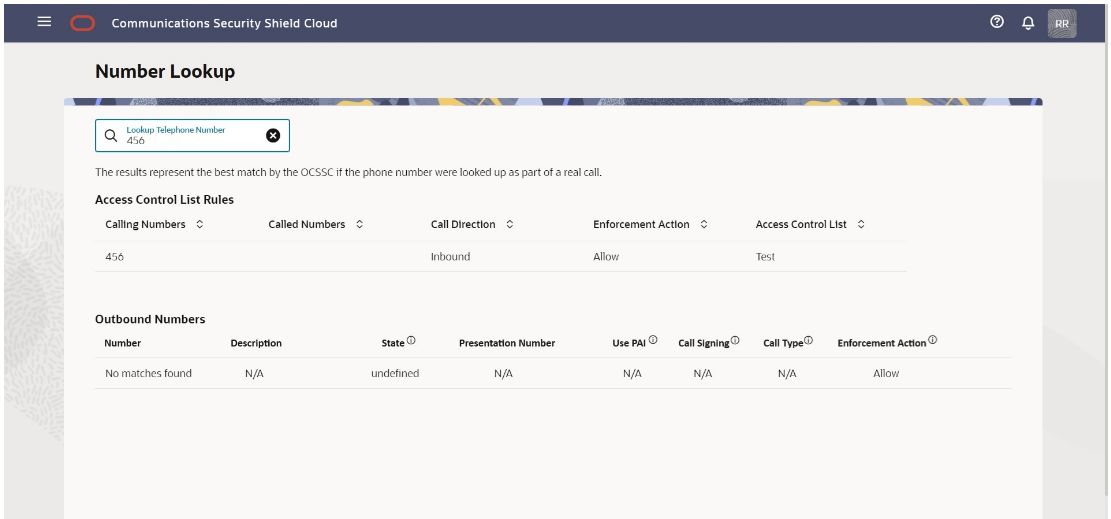
Outbound Numbers

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Enforcement Action
12345		Active	34545	Yes	N/A	None	Allow

Phone Number Configured in the Access Control List Rules and is Not Configured in the Outbound Numbers List

When you look up a number that is configured in the Access Control List Rules and is not configured in the Outbound Numbers, the results show the phone number only in the Access Control List and displays the following information.

- Access Control List Rules—The results also show the configured call direction, enforcement action, and the name of the Access Control List that includes the number.
- Outbound Numbers—The results show "No matches found" and the enforcement action that the user configured for "Outbound Calling Numbers Not Configured" on the General Settings page on the Outbound Numbers page.



Number Lookup

Lookup Telephone Number
456

The results represent the best match by the OCSSC if the phone number were looked up as part of a real call.

Access Control List Rules

Calling Numbers	Called Numbers	Call Direction	Enforcement Action	Access Control List
456		Inbound	Allow	Test

Outbound Numbers

Number	Description	State	Presentation Number	Use PAI	Call Signing	Call Type	Enforcement Action
No matches found	N/A	undefined	N/A	N/A	N/A	N/A	Allow

Look Up a Phone Number on the Security Shield Number Lookup Page

When you want to see all Oracle® Communications Security Shield Cloud Service (Security Shield) lists that contain a phone number, use the Number Lookup page. The results represent the best match by Security Shield if the phone number were looked up as part of a real call.

Before You Begin

- Add phone numbers to the Security Shield list types.

Procedure
In the following procedure, the phone number you enter must contain either 1-32 digits or use the E.164 format. Number Lookup does not support the use of wild cards.

> **Note:**
>
> When you leave the Number Lookup page after entering a phone number to look up, Security Shield clears the Telephone Number field.

1. Access the **Number Lookup** page.
2. In the **Lookup Telephone Number** field enter the number you want to find, and press **Enter**.

   Security Shield displays the phone number in each type of list that includes it along with its settings.

10
Activity Logs

Oracle® Communications Security Shield Cloud Service (Security Shield) Activity logs provide a view of user activity to help with troubleshooting and audits. You can see logged activity such as configuration changes to access control lists, threshold parameters, and on-premises software components.

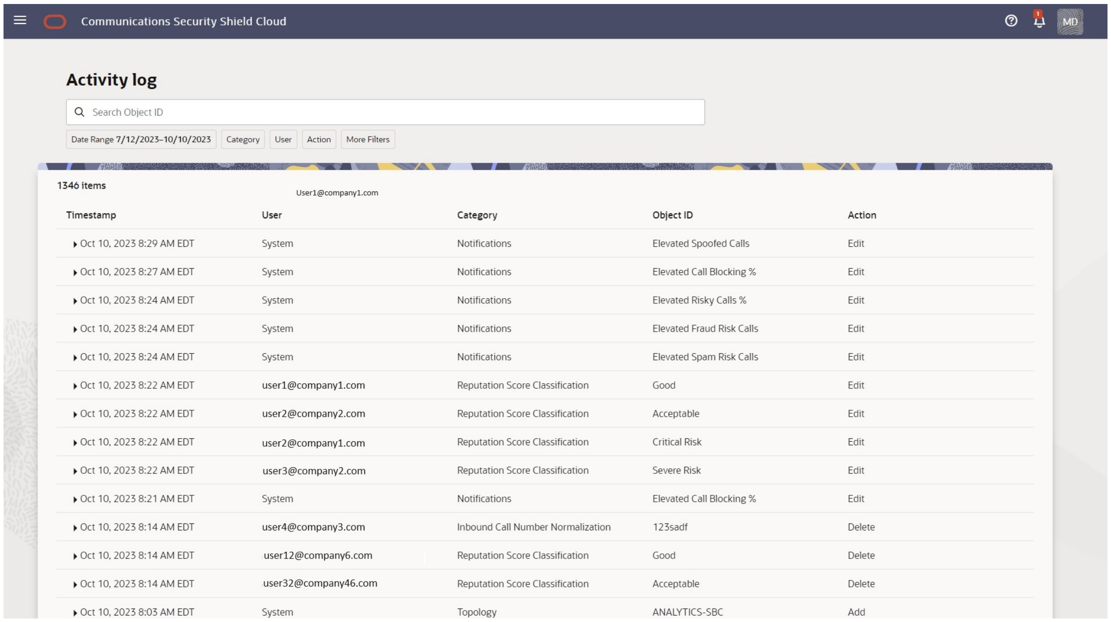
Topics:

- Activity Log Controls and Actions
- Search the Activity Log Using Filter Chips
- Search the Activity Log Using the Object ID

Activity Log Controls and Actions

The Oracle® Communications Security Shield Cloud Service (Security Shield) Activity Log displays logged information in categories, which you can search for details. Security Shield creates the logs while registering a Session Border Controller (SBC) or the Cloud Communication Service (CCS) or when unregistering an SBC or CCS for a tenant.

The following screen capture shows the Activity Log page. The Activity Log can display up to 1,050 logs, which you can view by scrolling down the table.



Activity log

Date Range 7/12/2023–10/10/2023

1346 items

User1@company1.com

Timestamp	User	Category	Object ID	Action
Oct 10, 2023 8:29 AM EDT	System	Notifications	Elevated Spoofed Calls	Edit
Oct 10, 2023 8:27 AM EDT	System	Notifications	Elevated Call Blocking %	Edit
Oct 10, 2023 8:24 AM EDT	System	Notifications	Elevated Risky Calls %	Edit
Oct 10, 2023 8:24 AM EDT	System	Notifications	Elevated Fraud Risk Calls	Edit
Oct 10, 2023 8:24 AM EDT	System	Notifications	Elevated Spam Risk Calls	Edit
Oct 10, 2023 8:22 AM EDT	user1@company1.com	Reputation Score Classification	Good	Edit
Oct 10, 2023 8:22 AM EDT	user2@company2.com	Reputation Score Classification	Acceptable	Edit
Oct 10, 2023 8:22 AM EDT	user2@company1.com	Reputation Score Classification	Critical Risk	Edit
Oct 10, 2023 8:22 AM EDT	user3@company2.com	Reputation Score Classification	Severe Risk	Edit
Oct 10, 2023 8:21 AM EDT	System	Notifications	Elevated Call Blocking %	Edit
Oct 10, 2023 8:14 AM EDT	user4@company3.com	Inbound Call Number Normalization	123sadf	Delete
Oct 10, 2023 8:14 AM EDT	user12@company6.com	Reputation Score Classification	Good	Delete
Oct 10, 2023 8:14 AM EDT	user32@company46.com	Reputation Score Classification	Acceptable	Delete
Oct 10, 2023 8:03 AM EDT	System	Topology	ANALYTICS-SBC	Add

Activity Log Triggers

The system creates logs for the following events:

- Call Type Classifications and Reputation Score Classifications—When a user changes the enforcement action.

- Access Control Lists—When a user creates, edits, or deletes and Access Control List.
- Notifications—When a user enables or disables notifications and when the system triggers alerts.
- Automatic Threat Protection—When a user updates thresholds.
- Outbound Number Management—When a user modifies outbound numbers and settings.
- Number Normalization—When a user enables or disables number normalization fields.

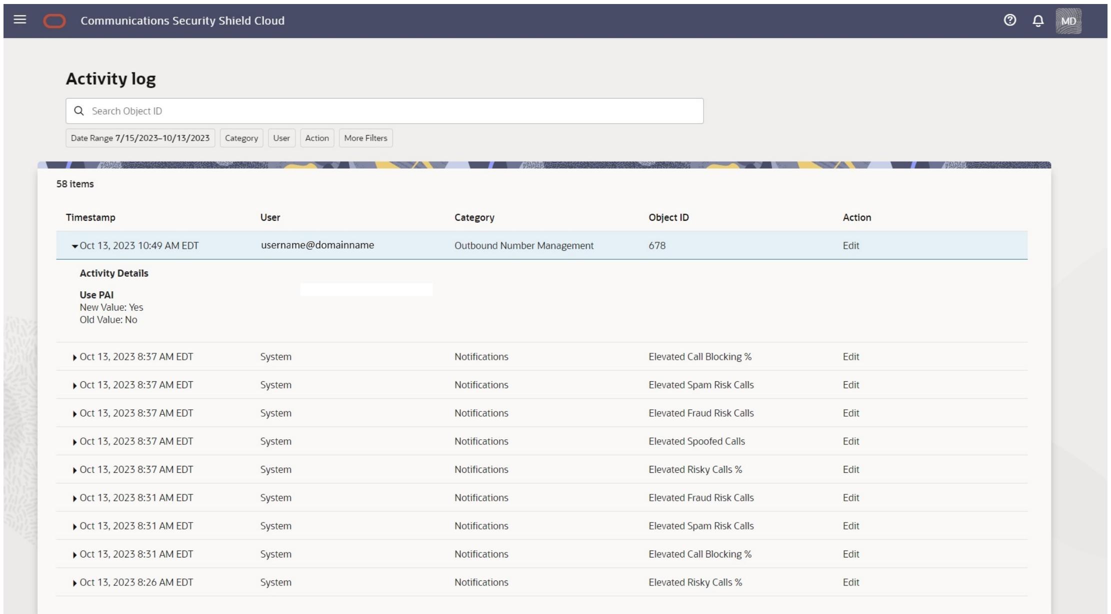
Activity Log Column Descriptions

The Activity Log shows the following information sorted by timestamps in ascending order in a scrollable list.

- Timestamp—Shows the date, time, and time zone of the log entry.
- User—Shows the name or email address of the user who performed the action on the date of the timestamp.
- Category—Shows the log category. Access Control Lists | Autonomous Threat Protection | Reputation Score Classification | Configuration Wizard.
- Object ID—Shows the name of the affected object within the Category, for example, a phone number on an Access Control List or an enforcement action on a Telemarketing Call Classification.
- Action—Shows the action performed on the affected object. Add | Edit | Delete.
- Activity Details—Shows the details of the action performed on the object, including both the former value and new value. Click the twister control to the left of the Timestamp to see Activity Details.

> **Note:**
>
> You cannot remove an activity log. Only the system can remove an activity log, which occurs when the maximum number of logs accrues (100,000).

The following screen capture shows an example of an expanded log, showing the Activity Details. The Activity Details show the name of the affected configuration parameter, which is Use PAI in this example, and the Old and New values for the parameter.



Communications Security Shield Cloud

Activity log

Search Object ID

Date Range 7/15/2023–10/13/2023 | Category | User | Action | More Filters

58 items

Timestamp	User	Category	Object ID	Action
Oct 13, 2023 10:49 AM EDT	username@domainname	Outbound Number Management	678	Edit
Oct 13, 2023 8:37 AM EDT	System	Notifications	Elevated Call Blocking %	Edit
Oct 13, 2023 8:37 AM EDT	System	Notifications	Elevated Spam Risk Calls	Edit
Oct 13, 2023 8:37 AM EDT	System	Notifications	Elevated Fraud Risk Calls	Edit
Oct 13, 2023 8:37 AM EDT	System	Notifications	Elevated Spoofed Calls	Edit
Oct 13, 2023 8:37 AM EDT	System	Notifications	Elevated Risky Calls %	Edit
Oct 13, 2023 8:31 AM EDT	System	Notifications	Elevated Fraud Risk Calls	Edit
Oct 13, 2023 8:31 AM EDT	System	Notifications	Elevated Spam Risk Calls	Edit
Oct 13, 2023 8:31 AM EDT	System	Notifications	Elevated Call Blocking %	Edit
Oct 13, 2023 8:26 AM EDT	System	Notifications	Elevated Risky Calls %	Edit

Activity Details

Use PAI
New Value: Yes
Old Value: No

The Activity Log builds the results of searches dynamically, where the search results show only users and categories for which a logged event occurred. For example, suppose you search for UsernameAbcd@companynameXyz.com and UsernameAbcd@companynameXyz.com did not perform any logged event in the time frame you selected for your search. The results will not display UsernameAbcd@companynamexyzin the results list. The same behavior applies to searching by category, where the results display only the categories in which a logged event occurred.

Multiple Users and Log Viewing

When User1 is viewing the Activity Log and User2 makes changes to a configuration, User1 does not immediately see the changes. User1 must refresh the table to see User2's changes.

Search the Activity Log Using Filter Chips

To help you find logs, the Oracle® Communications Security Shield Cloud Service (Security Shield) Activity Log tab displays a set of filter chips that you move to the Search field to help narrow your search.

Procedure

You can set multiple filters and you can change or clear them, as needed.

> **Note:**
>
> The Search with filters function does not support saving searches.

1. Access the **Activity Log** page.
2. Move one or more of the filter chips into the Search field.
   - Date Range—Click the chip to display the date range picker, where you set a custom date range.
   - User—Click the chip to display a list of users and select a user.

- Category—Click the chip to display a list of categories and select one or more categories. Choices: Topology | Reputation Score Classification | Access Control List | Notifications | Inbound Call Number Normalization
- Action—Click the chip to display a list of actions and select one or more actions. Valid Values: Add | Edit | Delete.
- More Filters—Click the chip to display a list of fixed time frames for the search. Valid Values: Last 24 Hours | Last 7 Days | Last 30 Days.

3. View the logs and click the twister by the timestamps to see the details of each one.

Search the Activity Log Using the Object ID

At the top of the page, the Activity Log tab displays the Search field to help you find activity logs for a certain object that the Oracle® Communications Security Shield Cloud Service (Security Shield) logs. The term "Object" can refer to a call classification type, the name of a system in your network, an Anonymous Threat Protection setting, a phone number, or the name of an Access Control List.

Before You Begin

- Find the object ID, such as the name of an object within the Category, for example, a phone number on an Access Control List, or an enforcement action on a Telemarketing Call Classification.

Procedure
Use the following procedure to save time searching when you know the Object ID.

1. Access the **Activity Log** page.
2. In the **Search Object ID** field, enter the Object ID. The field is not case sensitive.

   Security Shield displays the results in a list that you can scroll.

11 Notifications

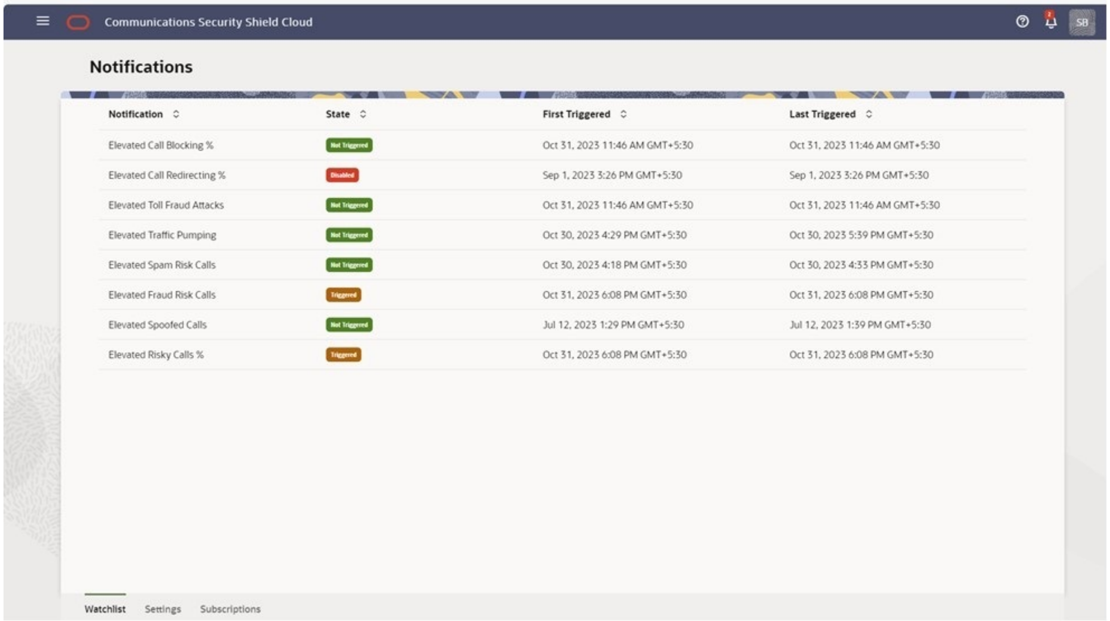
Oracle® Communications Security Shield Cloud Service (Security Shield) Notifications displays notifications when certain conditions occur that need your attention. On the Notifications page, privileged users can view the state of risky call types and manage notifications settings.

Topics:

Notifications Controls and Actions

The Notifications page displays tabs where you can view the notifications watch list, manage call enforcement notifications, and manage your subscriptions.

The following screen capture shows the Notifications and its tabs.



Notifications

Notification	State	First Triggered	Last Triggered
Elevated Call Blocking %	Not Triggered	Oct 31, 2023 11:46 AM GMT+5:30	Oct 31, 2023 11:46 AM GMT+5:30
Elevated Call Redirecting %	Disabled	Sep 1, 2023 3:26 PM GMT+5:30	Sep 1, 2023 3:26 PM GMT+5:30
Elevated Toll Fraud Attacks	Not Triggered	Oct 31, 2023 11:46 AM GMT+5:30	Oct 31, 2023 11:46 AM GMT+5:30
Elevated Traffic Pumping	Not Triggered	Oct 30, 2023 4:29 PM GMT+5:30	Oct 30, 2023 5:39 PM GMT+5:30
Elevated Spam Risk Calls	Not Triggered	Oct 30, 2023 4:18 PM GMT+5:30	Oct 30, 2023 4:33 PM GMT+5:30
Elevated Fraud Risk Calls	Triggered	Oct 31, 2023 6:08 PM GMT+5:30	Oct 31, 2023 6:08 PM GMT+5:30
Elevated Spoofed Calls	Not Triggered	Jul 12, 2023 1:29 PM GMT+5:30	Jul 12, 2023 1:39 PM GMT+5:30
Elevated Risky Calls %	Triggered	Oct 31, 2023 6:08 PM GMT+5:30	Oct 31, 2023 6:08 PM GMT+5:30

Security Shield can send direct communication by email, Slack, and PagerDuty when notifications occur. The banner displays a counter on the bell icon when notifications occur, as shown in the following screen capture.

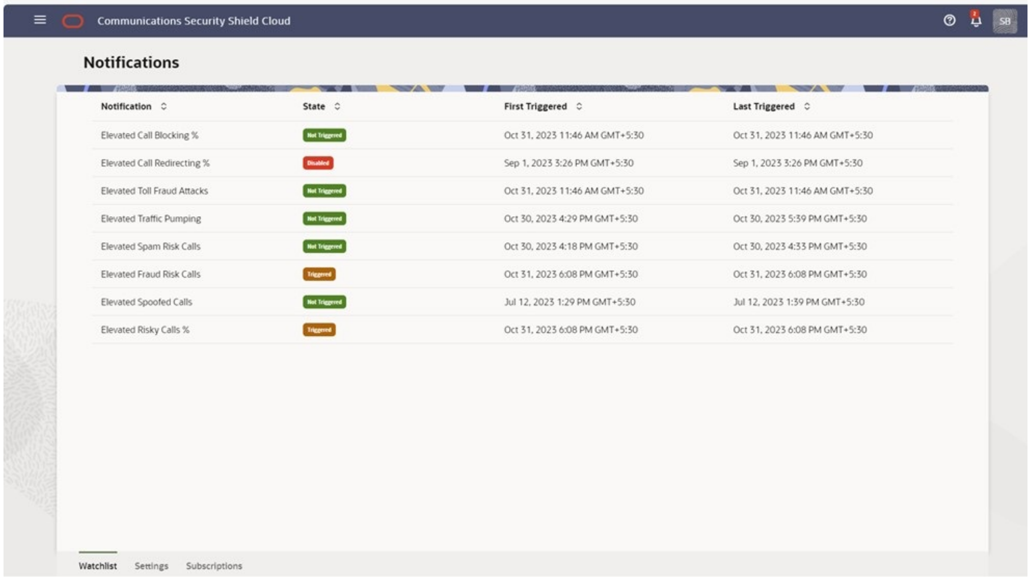
Note:

The notifications counter (on the bell icon on the banner) shows the number of notifications currently triggered, not the number of notifications since the last time you viewed the notifications list.

The Notifications Watchlist Tab

The Notifications Watchlist tab displays the list of notification types that Oracle® Communications Security Shield Cloud Service (Security Shield) provides along with their state and trigger times.

The following screen capture shows an example of the Notifications Watchlist tab.



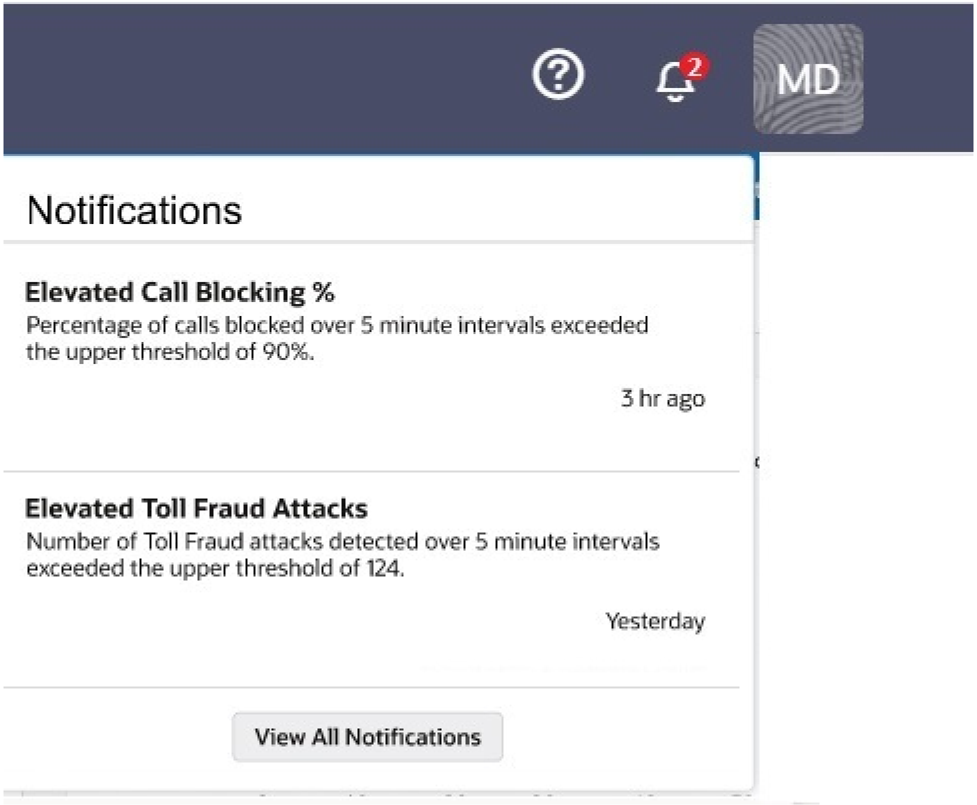
Notification	State	First Triggered	Last Triggered
Elevated Call Blocking %	Not Triggered	Oct 31, 2023 11:46 AM GMT+5:30	Oct 31, 2023 11:46 AM GMT+5:30
Elevated Call Redirecting %	Disabled	Sep 1, 2023 3:26 PM GMT+5:30	Sep 1, 2023 3:26 PM GMT+5:30
Elevated Toll Fraud Attacks	Not Triggered	Oct 31, 2023 11:46 AM GMT+5:30	Oct 31, 2023 11:46 AM GMT+5:30
Elevated Traffic Pumping	Not Triggered	Oct 30, 2023 4:29 PM GMT+5:30	Oct 30, 2023 5:39 PM GMT+5:30
Elevated Spam Risk Calls	Not Triggered	Oct 30, 2023 4:18 PM GMT+5:30	Oct 30, 2023 4:33 PM GMT+5:30
Elevated Fraud Risk Calls	Triggered	Oct 31, 2023 6:08 PM GMT+5:30	Oct 31, 2023 6:08 PM GMT+5:30
Elevated Spoofed Calls	Not Triggered	Jul 12, 2023 1:29 PM GMT+5:30	Jul 12, 2023 1:39 PM GMT+5:30
Elevated Risky Calls %	Triggered	Oct 31, 2023 6:08 PM GMT+5:30	Oct 31, 2023 6:08 PM GMT+5:30

The Notifications Watchlist reports three possible states for the notifications.

- Triggered – Calls exceeded the upper threshold you set for triggering the notification. When calls fall below the lower threshold you set, the state changes to Not Triggered.
- Not Triggered – Calls did not exceed the upper threshold you set for triggering the notification. When calls exceed the upper threshold you set, the state changes to Triggered.
- Disabled – The notification is disabled.

Security Shield updates the Notifications Watchlist every five minutes. Notifications age out when the source falls below the lower threshold you set. Because you might not see notifications occurring over a weekend, for example, the default age-out is twenty four hours. When a notification ages out, Security Shield no longer counts the notification as an active notification but the notifications list still includes the notification.

When the notifications counter displays digits on the bell icon. Click the bell and Security Shield displays the Notifications list, as shown in the following example.



Notifications

Elevated Call Blocking %
Percentage of calls blocked over 5 minute intervals exceeded the upper threshold of 90%.

3 hr ago

Elevated Toll Fraud Attacks
Number of Toll Fraud attacks detected over 5 minute intervals exceeded the upper threshold of 124.

Yesterday

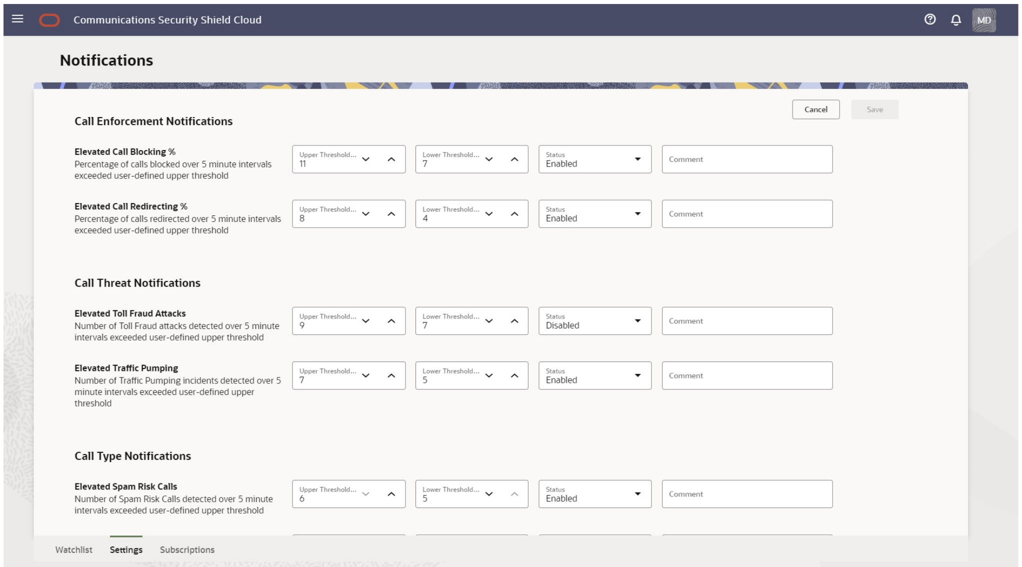
Note:

The counter shows the number of notifications currently triggered, not the number of notifications since the last time you viewed the notifications list.

The Notifications Settings Tab

The Oracle® Communications Security Shield Cloud Service (Security Shield) Settings tab displays predefined notifications you can enable or disable. You can also set the thresholds for triggering and clearing the notifications. All notifications default to disabled and all thresholds default to no setting.

The following screen capture shows the notifications with descriptions and the parameters you can set.



Communications Security Shield Cloud

MD

Notifications

Cancel

Save

Call Enforcement Notifications

Elevated Call Blocking %
Percentage of calls blocked over 5 minute intervals exceeded user-defined upper threshold

Upper Threshold... 11 | Lower Threshold... 7 | Status Enabled | Comment

Elevated Call Redirecting %
Percentage of calls redirected over 5 minute intervals exceeded user-defined upper threshold

Upper Threshold... 8 | Lower Threshold... 4 | Status Enabled | Comment

Call Threat Notifications

Elevated Toll Fraud Attacks
Number of Toll Fraud attacks detected over 5 minute intervals exceeded user-defined upper threshold

Upper Threshold... 9 | Lower Threshold... 7 | Status Disabled | Comment

Elevated Traffic Pumping
Number of Traffic Pumping incidents detected over 5 minute intervals exceeded user-defined upper threshold

Upper Threshold... 7 | Lower Threshold... 5 | Status Enabled | Comment

Call Type Notifications

Elevated Spam Risk Calls
Number of Spam Risk Calls detected over 5 minute intervals exceeded user-defined upper threshold

Upper Threshold... 6 | Lower Threshold... 5 | Status Enabled | Comment

Upper Threshold—The point at which Security Shield triggers the notification.

Lower Threshold—The point at which Security Shield clears the notification.

Status—Whether or not the notification is enabled.

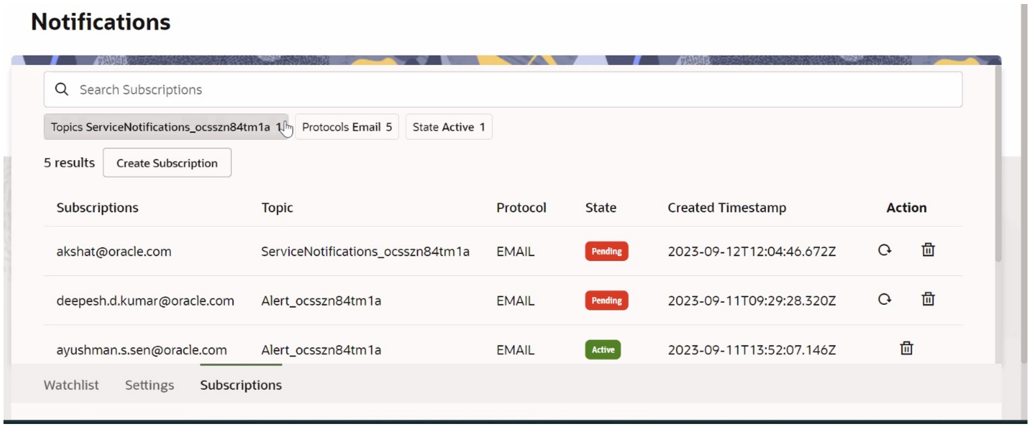
Comment—Enter any notes you might want, for example, why you enabled or disabled a notification or why you set the thresholds to certain levels.

The settings take effect when you click **Save**.

The Notifications Subscriptions Tab

The Subscriptions tab on the Oracle® Communications Security Shield Cloud Service (Security Shield) Notifications page displays information about the subscribers configured to receive notifications when Security Shield detects threat conditions. The Subscriptions tab also displays the Create Subscription button to launch the configuration drawer, as well as filter chips for search operations.

The subscriptions tab displays filter chips you can use for search and lists your subscribers along with the Alert type, Protocol, Active Status, and Creation Timestamp. In the Search field, you can also enter all or part of Topic to see a list of only those subscribers.



Notifications

Search Subscriptions

Topics ServiceNotifications_ocsszn84tm1a 1 | Protocols Email 5 | State Active 1

5 results | Create Subscription

Subscriptions	Topic	Protocol	State	Created Timestamp	Action
akshat@oracle.com	ServiceNotifications_ocsszn84tm1a	EMAIL	Pending	2023-09-12T12:04:46.672Z	
deepesh.d.kumar@oracle.com	Alert_ocsszn84tm1a	EMAIL	Pending	2023-09-11T09:29:28.320Z	
ayushman.s.sen@oracle.com	Alert_ocsszn84tm1a	EMAIL	Active	2023-09-11T13:52:07.146Z	

Definitions of the Columns and Filter Chips

Subscription—The delivery endpoint where Security Shield sends published messages for a particular topic. See Slack and PagerDuty for hooks and integration information. Every message sent out as email contains a link to unsubscribe from the related topic, so Subscribers can unsubscribe themselves from notifications. Only the Privileged Administrator can unsubscribe recipients from HTTPS and Slack notifications. Security Shield updates the subscription list whenever a change is made to the list or when you navigate to the Subscription tab.

Topic—A channel for communicating messages to a subscription. The only topic supported at this time is Alert.

Protocol—The means for delivering notifications to subscriptions. Security Shield can send notifications to:

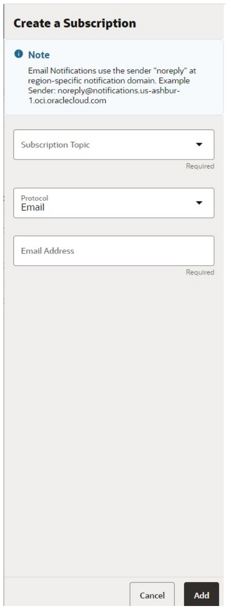
- Email—An email address
- HTTPS—PagerDuty
- Slack—A Slack channel

State—The availability of the subscriber to receive notifications. Active means the subscriber will receive notifications. Pending means Security Shield notified the subscriber about the subscription, but the subscriber has not yet clicked the link in the notification required to activate the subscription.

Created Time Stamp—The day, year, and time when the Privileged User created the subscription.

Create A Notification Subscription

The **Create Subscription** button launches the Create Subscription configuration drawer where Privileged Users configure Security Shield to send notifications to designated subscribers by way of email, Slack, and PagerDuty services when call threats occur.



Create a Subscription

Note

Email Notifications use the sender "noreply" at region-specific notification domain. Example Sender: noreply@notifications.us-ashbur-1.oci.oraclecloud.com

Protocol: Email

Remove Subscriptions

Security Shield provides the following methods for removing subscriptions.

- Privileged Users can remove email, Slack, and PagerDuty subscriptions. See Unsubscribe Users From Notifications
- Subscribers can only Unsubscribe from email notifications, Subscribers use the link included in every notification sent by email.

Notifications Subscriptions Behavior and Configuration Guidelines

Notifications from Oracle® Communications Security Shield Cloud Service (Security Shield) can alert end-users you configure about potentially harmful threats detected by Security Shield. The following information describes how the notifications work.

On the Notifications Settings Tab, Privileged Users can configure settings for triggering and ending specific types of notifications about potentially harmful call-traffic events. On The Notifications Subscriptions Tab, privileged users can Configure Subscriptions to Notifications for the end-users (called subscribers) you want to receive the notifications.

> **Note:**
>
> You cannot alter the messages sent in notifications.

Security Shield attempts to deliver notifications as soon as they occur and applies no restriction on the number of messages pushed out. Security Shield can deliver up to ten email messages per minute and up to sixty transactions per minute per alert type (called a Topic). Security Shield delivers each message at least once per subscription.

> **Note:**
>
> Security Shield notifications supports only one topic (named Alert) at this time.

Notifications support the following:

- up to ten endpoints per topic, which can be a combination of multiple email addresses, one Slack endpoint, and one PagerDuty endpoint.
- up to ten email addresses when you set no Slack and PagerDuty endpoints.
- only one Slack endpoint per topic.
- only one PagerDuty endpoint per topic.
- a group email address as the endpoint.

After you configure a subscriber to receive notifications, the subscriber must activate the subscription. The configuration and activation process includes the following steps and results:

1. Access the Notifications page and go to the Subscriptions tab.

2. Configure one or more subscribers whom you want to receive notifications. Security Shield sends a confirmation email to the subscriber that contains a confirmation link and also lists the subscriber on the Subscription table as Pending.
3. The subscriber must click the activation link in the email to activate the subscription. When the subscription becomes active, the Subscription table reports the State as Active.

See Slack and PagerDuty for integration information.

Security Shield Threat Notifications Messages

You can configure Oracle® Communications Security Shield Cloud Service (Security Shield) to send notifications about detected threat conditions by way of email, Slack, and PagerDuty to designated subscribers. Notifications occur when the alert state for a call type changes from Not Triggered to Triggered, according to the thresholds you set.

Notifications include messages that Security Shield publishes to a topic, for example, Alerts. (A topic is a channel for communicating messages to a subscription.) Security Shield delivers each message at least once per subscription. Every email message contains a link to unsubscribe from the related topic. The following table lists and describes the information Security Shield provides for the Alerts topic.

> **Note:**
>
> You cannot edit the content of the messages.

Alert Category	Alert Name	Message
Call Enforcement	Elevated Call Blocking %	Title: Security Shield Alert: Higher number blocked calls than expected Message: [Trigger time stamp]. The number of blocked calls exceeded your configured threshold. Please investigate the reason for the number of blocked calls. You may want to reconfigure Security Shield to prevent blocking calls you want.
	Elevated Call Redirecting %	Security Shield Alert: High Number of redirected calls than expected [Trigger time stamp]. The number of redirected calls exceeded your configured threshold. The increase may indicate an attack. Please investigate the reason for the number of redirected calls. You may want to reconfigure Security Shieldto prevent redirecting calls you want.

Alert Category	Alert Name	Message
Toll Fraud	Elevated Toll Fraud Attacks	Security Shield Alert: Suspected Fraud on outbound calls. [Trigger time stamp]. Security Shield detected a possible attack against your voice infrastructure from fraudulent outbound calls. Fraudulent outbound calls may result in higher charges from your service provider. Oracle recommends blocking toll fraud calls.
Traffic Pumping Attacks	Elevated Traffic Pumping Attacks	Security Shield Alert: Security Shield Higher number of calls than expected; possible call flooding detected [Trigger time stamp]. Security Shield detected a possible attack against your voice infrastructure using inflated traffic volumes. Call flooding from traffic pumping may result in service impairment. Your customers may experience difficulty in getting through. Monitor the situation. Oracle recommends throttling traffic pumping calls.
Call Type	Elevated Spam Risk Calls	Security Shield Alert: More SPAM calls than expected. High number of suspected SPAM calls. [Trigger time stamp]. The number of suspected SPAM calls exceeded the configured threshold. The result may impair service and cause productivity loss. Monitor the situation. If needed, block or throttle SPAM calls until the numbers drop to more normal levels.
	Elevated Fraud Risk Calls	Security Shield Alert: Suspected fraud calls [Trigger time stamp]. The number of suspected fraudulent calls exceed the configured threshold. The increase may indicate an attack on your service. Monitor the situation. If needed, block or redirect fraud calls until the numbers drop to more normal levels.

Alert Category	Alert Name	Message
	Elevated Spoofed Calls	Security Shield Alert: Higher numbers of spoofed calls than expected. [Trigger time stamp]. The number of suspected spoofed calls exceeded the configured threshold. The increase may indicate a reconnaissance attack, phishing attack, or other malicious behavior. Monitor the situation. If needed, block or throttle spoofed calls until the numbers drop to more normal levels.
Call Classification	Elevated Risky Calls %	Security Shield Alert: Higher number of Risky calls than expected [Trigger time stamp]. The number of risky calls exceeded the configured threshold. Security Shield detected very suspicious behavior. Monitor the situation. If needed, block, redirect, or throttle the highest risk categories until the numbers drop to more normal levels.

Configure Subscriptions to Notifications

Privileged users can configure Oracle® Communications Security Shield Cloud Service (Security Shield) to send notifications to designated subscribers about threat conditions that Security Shield detects. You can specify sending notifications by email, Slack, and PagerDuty services.

Procedure
In the following procedure, you set the subscription topic, protocol, and endpoints. You can set...

- up to ten endpoints per topic, which can be a combination of multiple email addresses, one Slack endpoint, and one PagerDuty endpoint.
- up to ten email addresses when you set no Slack and PagerDuty endpoints.
- only one Slack endpoint per topic.
- only one PagerDuty endpoint per topic.
- a group address for the email endpoint.

Before You Begin

- Confirm that you are assigned to the Security Shield Configuration Editor and Security Shield Administrator roles.

1. Access the **Notifications** page and click the **Subscriptions** tab.
2. On the Subscription tab, click **Create Subscription**.

3. In the Create Subscription dialog, do the following:
    - Subscription Topic—Select **Alert**. Security Shield supports no other topics at this time.
    - Protocol—Select the service you want Security Shield to use to send notifications. Default: Email. Valid values: Email | Slack | PagerDuty.
    - Enter the endpoint email, Slack URL, or PagerDuty integration key according to the protocol type you selected in the previous step. Endpoint configuration is case-sensitive.
4. Click **Add**.

    Security Shield adds the new subscriber to the subscription list table as Pending and emails a confirmation link to the subscriber.

Next Steps

- The new subscriber must click the link in the email to activate the subscription.

Unsubscribe Users From Notifications

Privileged Users can remove Subscribers from receiving Oracle® Communications Security Shield Cloud Service (Security Shield) notifications with the following procedure. Security Shield updates the subscription list whenever a change is made to the list or when you navigate to the subscription tab.

Before You Begin
Confirm you are assigned to the Privileged Users role.

Procedure
Use the following procedure for unsubscribing recipients from any delivery method through the Subscription tab.

1. Access the **Notifications** page and click the **Subscription** tab.
2. On the Subscription tab, locate the subscription to delete.
3. Click the **delete icon** at the end of the subscription row.

    Security Shield displays a confirmation dialog.
4. Click **Delete**.

    Security Shield removes the subscription.

User Groups Required for Managing Notifications

Users who want to view or manage Oracle® Communications Security Shield Cloud Service (Security Shield) Notifications must be assigned to the following user groups according to what they want to see or do.

Access the Notification List (View information)

- OCSS User
- OCSS ACL Editor
- OCSS Configuration Editor
- OCSS Device Configuration Editor

- OCSS User Tracking and Monitoring
- OCSS Administrator

Manage Notification Rules (Set thresholds)

- OCSS Configuration Editor
- OCSS Device Configuration Editor

Manage Notification State Changes (Enable-Disable)

- OCSS Administrator
- OCSS Device Configuration Editor

Enable Notifications and Set the Thresholds

Privileged Oracle® Communications Security Shield Cloud Service (Security Shield) users can enable and disable notifications, as well as set the triggering thresholds.

Before You Begin

- Confirm you are assigned to the OCSS Configuration Editor and OCSS Device Configuration Editor user groups to set thresholds for notifications.
- Confirm you are assigned to the OCSS User and OCSS Device Configuration Editor user groups to enable or disable notifications.

Procedure
You do not need to enable all notifications in a group. For example, in the Call Enforcement Notifications group you can enable Elevated Call Blocking and set Elevated Call Redirecting to disabled. Note that Security Shield does not set defaults for the threshold settings or status.

> **Note:**
>
> The Settings tab lists and describes the notifications you can configure.

1. Access the **Notifications** page and click the **Settings** tab.
2. On the Settings tab, set the following parameters for each notification type you want to use.
   - Upper Threshold—Set the threshold for turning notifications on. Valid values: 1-100 for percentages.1-20,000 for incidents.
   - Lower Threshold—Set the threshold for turning notifications off. Valid values: 1-100 for percentages.1-20,000 for incidents.
   - Status—Set to either enabled or disabled.
   - Comment—(Optional) Enter text, for example, to describe the purpose of the notification or why you want it disabled or enabled.
3. Click **Save**.

   The settings take effect right away.

12 Settings

The Oracle® Communications Security Shield Cloud Service (Security Shield) Settings page displays information that you need for installing the Cloud Communication Service and provides links to system-wide settings.

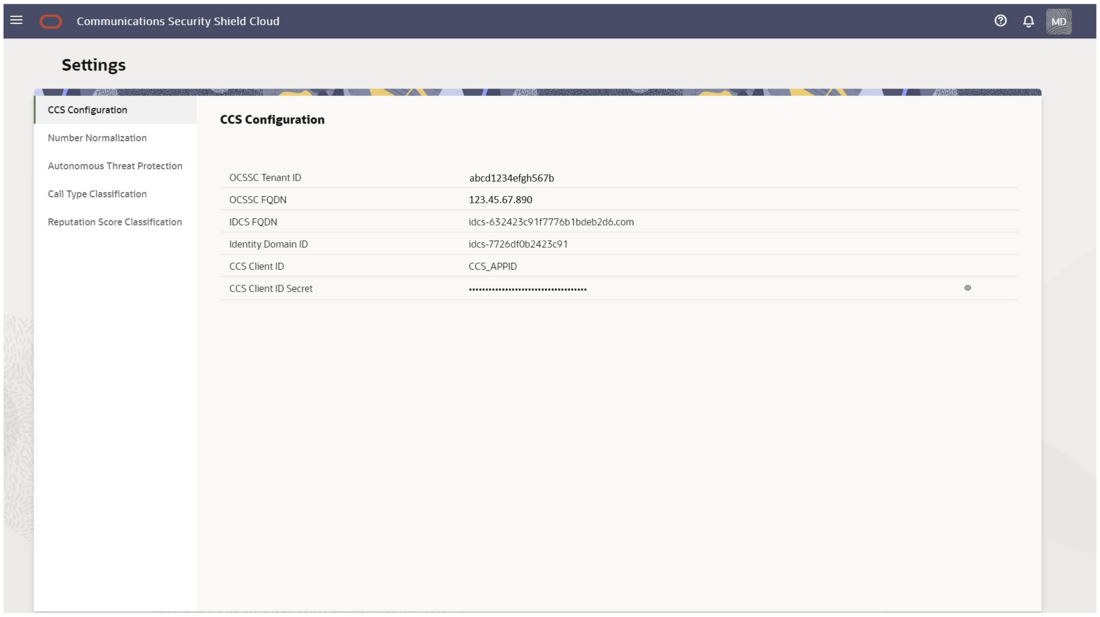
Topics:

- Settings Controls and Actions
- Cloud Communications Service Configuration Settings
- Inbound Calling Number Normalization Settings
- Autonomous Threat Protection Settings
- Call Type Classifications
- Reputation Score Classification

Settings Controls and Actions

Oracle® Communications Security Shield Cloud Service (Security Shield) Settings provides links to dialogs where you set thresholds, behaviors, and enforcement actions for call traffic. Before you install the Cloud Communication Service (CCS), refer to the CCS Configuration link which provides information that the CCS installation script requires you to supply.

The following screen capture shows the Settings landing page, which defaults to the CCS Configuration page.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification

CCS Configuration

OCSSC Tenant ID	abcd1234efgh567b
OCSSC FQDN	123.45.67.890
IDCS FQDN	idcs-632423c91f7776b1bdeb2d6.com
Identity Domain ID	idcs-7726df0b2423c91
CCS Client ID	CCS_APPID
CCS Client ID Secret	•••••••••••••••••••••••••••••••••••

CCS Configuration—Displays information that you need to provide when installing the Cloud Communication Service. (You cannot edit the information displayed here.)

Number Normalization—Displays a table of Inbound Calling Number Normalization rules. The system provides two default rules. You can create up to twenty-three more rules.

Autonomous Threat Protection—Displays configuration dialogs for configuring General (settings), Threat Vector Thresholds, and Domain Thresholds.

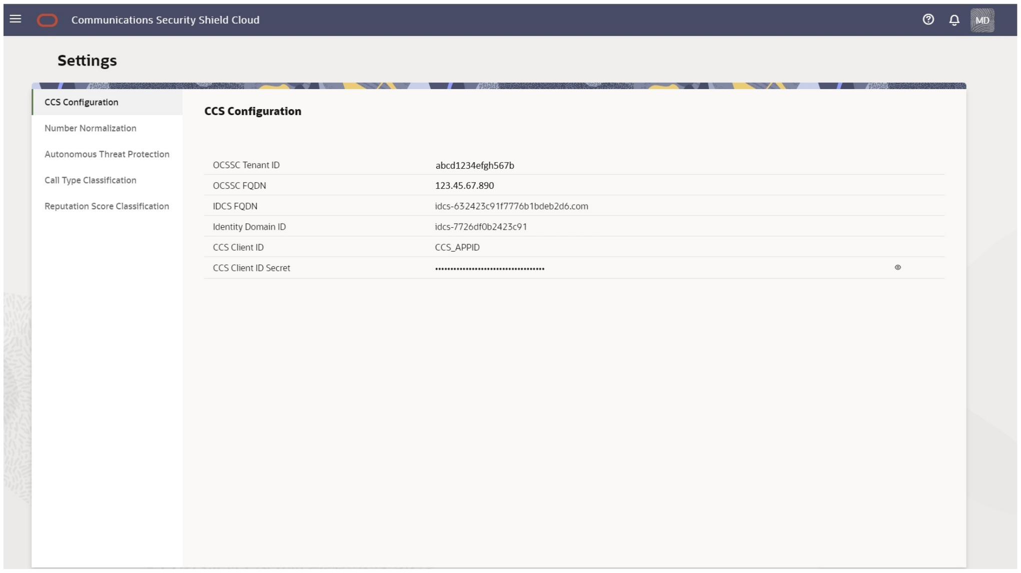
Call Type Classification—Displays descriptions of call type classifications and provides configurable enforcement settings.

Reputation Score Classification—Displays descriptions of reputation score classifications and provides configurable enforcement settings.

Cloud Communications Service Configuration Settings

When you download Oracle® Communications Security Shield Cloud Service (Security Shield) software and unpack the archive.tgz file, the system populates the CCS Configuration fields on the Settings page with information you need when you run the Cloud Communications Service (CCS) installation script.

Access the Settings page and click CCS Configuration to see the CCS Configuration page. The following screen capture shows the CCS Configuration page with sample configuration entries.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification

CCS Configuration

OCSSC Tenant ID	abcd1234efgh567b
OCSSC FQDN	123.45.67.890
IDCS FQDN	idcs-632423c91f7776b1bdeb2d6.com
Identity Domain ID	idcs-7726df0b2423c91
CCS Client ID	CCS_APPID
CCS Client ID Secret	••••••••••••••••••••••••••••••••••••

Note:

You cannot edit this page from Security Shield. Make edits through your Oracle Cloud Infrastructure (OCI) account.

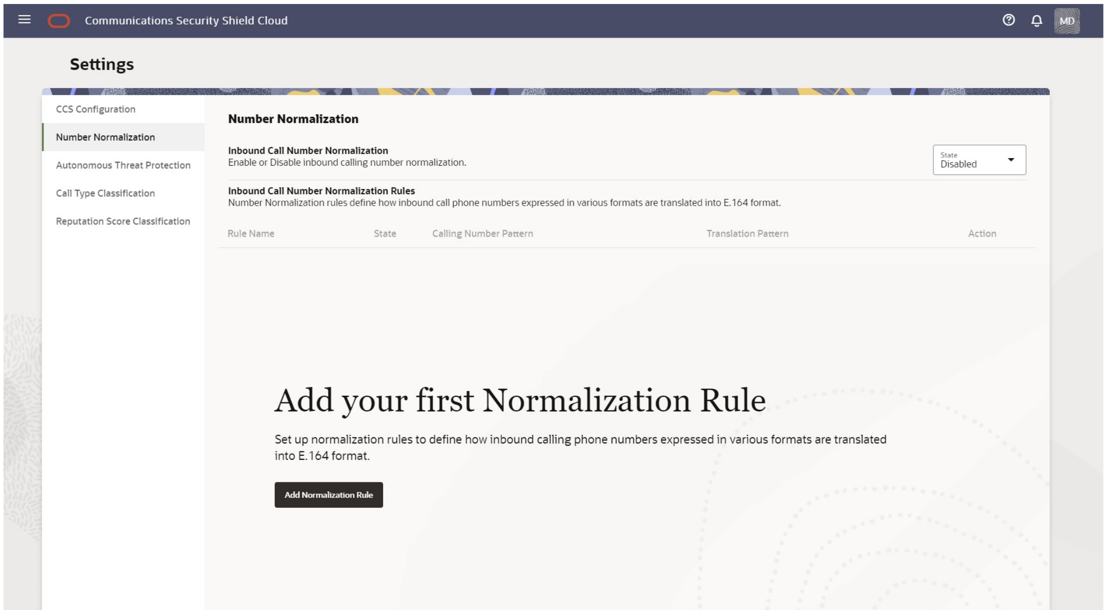
See "Install, Configure, and Activate the Cloud Communication Service" in the *Security Shield Installation and Maintenance Guide*.

Inbound Calling Number Normalization Settings

Oracle® Communications Security Shield Cloud Service (Security Shield) uses the E.164 format for phone numbers sent in the look-up API from the Oracle Communications Session Border Controller (SBC). Because Security Shield is often deployed in scenarios that use phone number formats other than E.164, Security Shield provides a way to normalize inbound calling numbers through translation rules.

Inbound calling number normalization rules translate phone numbers into the E.164 format when your SBC receives traffic that uses other phone number format conventions. Security Shield can normalize inbound phone numbers from multiple SIP trunk providers, as well. In this way, Security Shield can work with different countries, formats, and SIP Trunk providers.

To see the Number Normalization page, go to the Settings tab and click Number Normalization in the navigation pane. The following screen capture shows the Number Normalization page, which displays the Enable-Disable toggle and the Add Normalization Rule button. The following screen capture shows the Number Normalization page before any rules exist.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification

Number Normalization

Inbound Call Number Normalization
Enable or Disable inbound calling number normalization.

State: Disabled

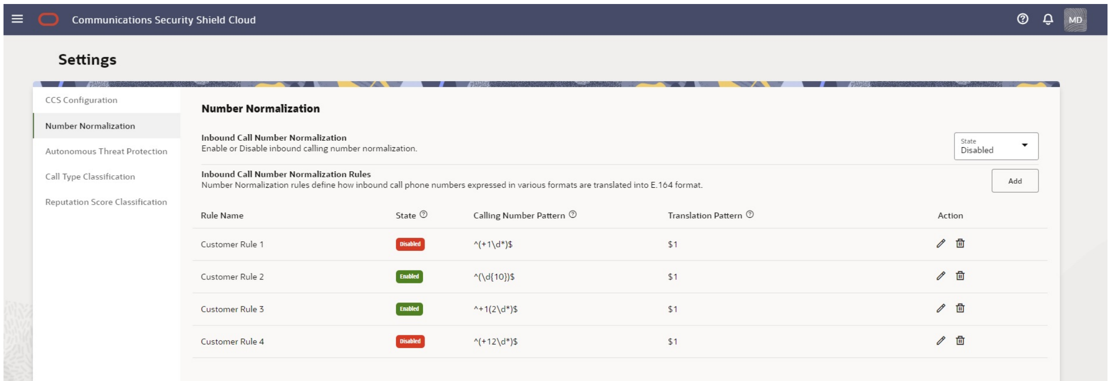
Inbound Call Number Normalization Rules
Number Normalization rules define how inbound call phone numbers expressed in various formats are translated into E.164 format.

Rule Name	State	Calling Number Pattern	Translation Pattern	Action

Add your first Normalization Rule

Set up normalization rules to define how inbound calling phone numbers expressed in various formats are translated into E.164 format.

The following screen capture shows the Number Normalization page with examples of entries. Depending on the number of entries, you may need to scroll to see all of them.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification

Number Normalization

Inbound Call Number Normalization
Enable or Disable inbound calling number normalization.

State: Disabled

Inbound Call Number Normalization Rules
Number Normalization rules define how inbound call phone numbers expressed in various formats are translated into E.164 format.

Rule Name	State	Calling Number Pattern	Translation Pattern	Action
Customer Rule 1	Disabled	^(+1\d*)$	$1	✎ 🗑
Customer Rule 2	Enabled	^(\d{10})$	$1	✎ 🗑
Customer Rule 3	Enabled	^+1(2\d*)$	$1	✎ 🗑
Customer Rule 4	Disabled	^(+12\d*)$	$1	✎ 🗑

The Number Normalization table columns include:

- Rule Name—Shows the list of rules in alphabetical order with no order of precedence for enforcement.
- State—Shows whether the rule is enabled or disabled. Regardless of the state, you can add, edit, and delete the rule.
- Calling Number Pattern—The regular expression that specifies a phone number for non-normalized inbound calling numbers that you want normalized into E.164 format. For example, the calling number pattern regular expression ^0(\d{6,9})$ describes phone numbers that start with 0 and are 7 to 10 digits long.
- Translation Pattern—The regular expression that specifies how to translate non-normalized inbound calling numbers that match the calling number pattern regular expression into E.164 format. The regular expression consists of Country Code to prepend (if specified) and $1. $1 captures the characters in the calling number regular expression included in side the parenthesis. For example, the translation pattern regular expression 31$1 adds a prefix of 31 to the captures (the phone number patterns characters in parenthesis.
- Action—The pencil icon displays the Edit Number Normalization Rule drawer where you specify the parameters of the rule. The trash can icon deletes the rule.

Using number normalization rules is optional, and Security Shield defaults to the disabled state. When no Number Normalization rule exists, Security Shield uses the calling number as received in either the FROM or PAI. When Number Normalization rules exist, Security Shield applies the rule to the calling number in the FROM and PAI. Phone number normalization works regardless of optional Header Manipulation Rules (HMR) on the Oracle Communications Border Controller that may manipulate the number.

Only a user assigned to the OCSS Configuration Editor role can add, edit, or delete phone Number Normalization rules. Security Shield supports up to twenty-five number normalization rules, including the two default rules.

> **Note:**
>
> The Activity log captures changes to number normalization and provides a filter called Inbound Call Number Normalization to help you find the changes.

See Syntax for Inbound Number Normalization Regular Expressions and Add New Inbound Phone Number Normalization Rules.

Default Inbound Calling Number Normalization Rules

Oracle® Communications Security Shield Cloud Service (Security Shield) provides two default inbound calling number normalization rules. A user assigned to the OCSS Configuration Editor role can enable, disable (default), and edit the rules.

International rule for North America and Caribbean

When the calling number of an inbound call includes an International Direct Dialing (IDD) prefix of 011, remove the 011 prefix. For example: translate 01144206555121 to 44206555121.

The Inbound Number Normalization Rules table displays the following information.

- Rule Name—International Inbound Calls in North America and Caribbean with 011 IDD Prefix (Remove IDD prefix)
- State—Enabled
- Calling Number Pattern—^011(\d*)$
- Translation Pattern—$1

National rule for North America and Caribbean

National rule for North America and Caribbean. When the calling number of an inbound call is a ten digit E.164 number, prepend it with 1. For example, translate 2065551212 to 12065551212.

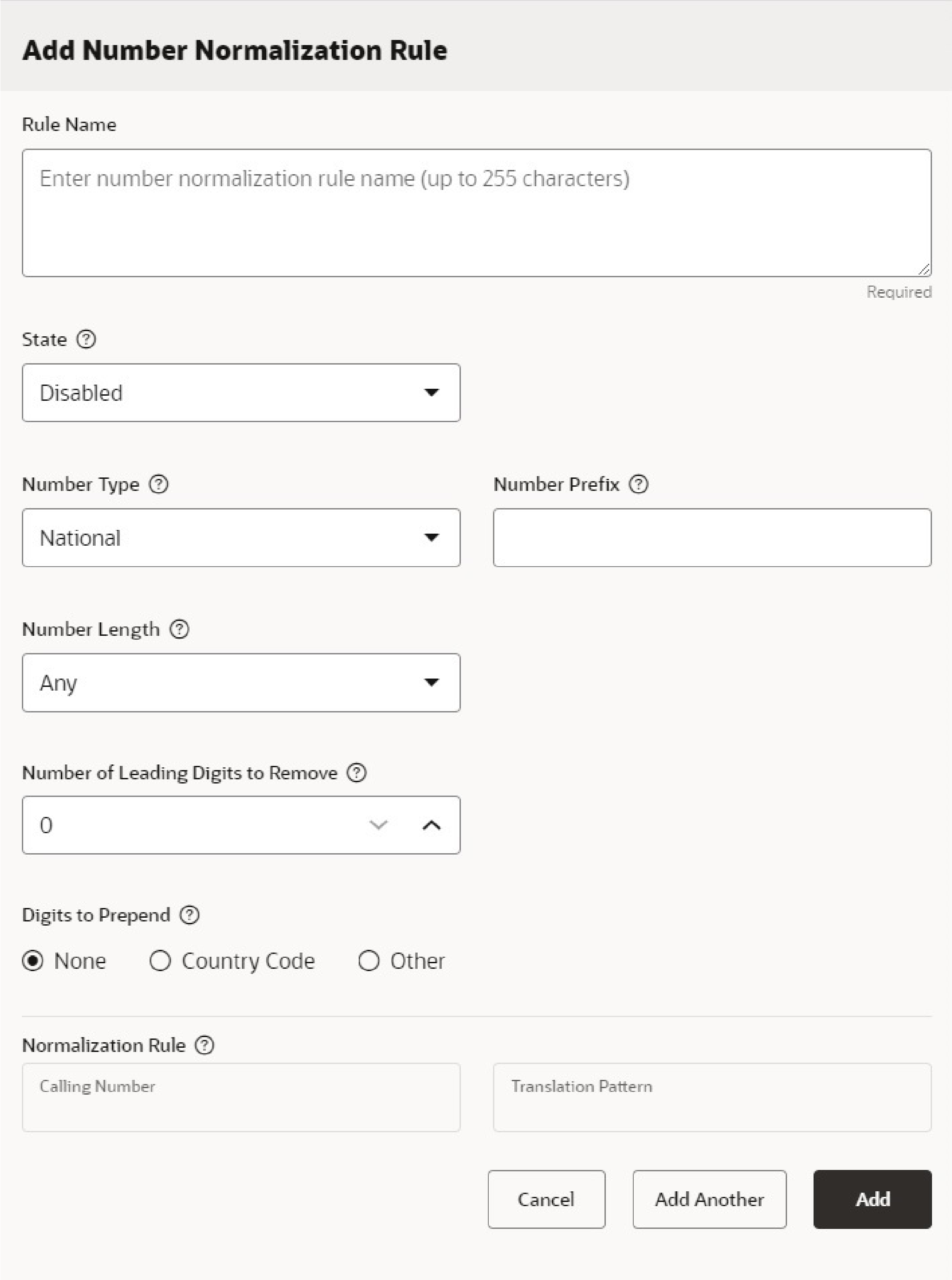
The Inbound Number Normalization Rules table displays the following information.

- Rule Name—North America and Caribbean Domestic Calls (Prepend 1)
- State—Enabled
- Calling Number Pattern—^(\d{10})$
- Translation Pattern—1$1

Inbound Calling Number Normalization Configuration Parameters

When you create a rule for inbound calling number normalization, Oracle® Communications Security Shield Cloud Service (Security Shield) uses the settings in the Add Number Normalization Rule drawer to create the regular expressions needed for normalizing phone numbers. You can add, edit, and delete rules with the service enabled or disabled.

The following screen capture shows the Add Number Normalization Rule drawer for creating Inbound Calling Number Normalization rules.



Add Number Normalization Rule

Rule Name

Enter number normalization rule name (up to 255 characters)

Required

State: Disabled

Number Type: National

Number Prefix:

Number Length: Any

Number of Leading Digits to Remove: 0

Digits to Prepend: ● None ○ Country Code ○ Other

Normalization Rule: Calling Number | Translation Pattern

Number Normalization Rule Configuration Parameters

Rule Name—The rule name can contain up to 255 characters, so you can make the name descriptive and unique. The table on the Number Normalization page lists the rules in alphabetical order. Security Shield enforces the rules in the following order of precedence:

State—The state of the rule, either enabled or disabled.

Number Type—The geographic scope of number you want normalized. Valid values: National | International.

- National—The dialog displays the Number Length and Digits to Prepend fields.
- International—The dialog hides the Number Length and Digits to Prepend fields.

Number Prefix—The leading digits (including the + character) of the inbound calling numbers that you want the calling number pattern to match.

Number Length—The length of the inbound calling numbers you want the call number pattern to match. You can specify the length of the number (including the + character) as any number, an exact number, or a range of numbers.

- When you select Range, the dialog displays counters for setting the minimum and maximum number of digits.
- When you select Exactly, the dialog displays a counter for setting the number.

Number of Leading Digits to Remove—The number of leading digits you want removed (including the + character).

Digits to Prepend—The digits you want Security Shield to add, if any, to the inbound calling number for translation into the E.164 format. Valid values:

- None—Hides the digits entry field.
- Country Code—Displays the "Select Country" field and drop-down list.
- Other—Displays a blank field where you can enter 1-15 digits.

Calling Number Pattern—Not directly configurable. Shows the regular expression for capturing non-conforming inbound calling numbers that you want Security Shield to normalize into the E.164 format. Security Shield generates and displays the pattern in the Add and Edit dialogs as you configure the rule. For example, the calling number pattern regular expression ^0(\d{6,9})$ describes phone numbers that start with 0 and are 7 to 10 digits long.

Translation Pattern—Not directly configurable. Shows the regular expression for how to translate non-conforming inbound calling numbers that match the calling number pattern into the E.164 format. Security Shield generates and displays the pattern in the Add and Edit dialogs as you configure the rule. The regular expression consists of the Country Code or a 1-15 digit number (if specified) and $1. $1 captures the characters in the Calling Number Pattern regular expression included inside the parenthesis. For example, the translation pattern regular expression 31$1 adds a prefix of 31 to the captures (the phone number pattern characters in parenthesis), which translates the calling number 0206551212 to 31206551212.

> **Note:**
>
> Security Shield automatically generates both the Calling Number Pattern and Translation Pattern regular expressions as you configure the rule using the Number Prefix, Number Length, Number of Digits to Remove, and Country Code to Append values you specify. See Syntax for Inbound Number Normalization Regular Expressions.

Syntax for Inbound Number Normalization Regular Expressions

Oracle® Communications Security Shield Cloud Service (Security Shield) uses regular expressions to specify the patterns for inbound phone number normalization calling number matching and translation.

Security Shield automatically generates or updates the regular expressions for both the Calling Number pattern and Translation pattern from the Number Prefix, Number Length, Number of Digits to Remove, and Country Code to Append values that you specify when you Add New Inbound Phone Number Normalization Rules or Edit an Inbound Calling Number Normalization Rule. The following information describes the characters and syntax used in the regular expressions.

Regular Expression Syntax

Anchors

The regular expression uses anchor characters to match the beginning or end of a line.

- ^ Matches the start of a line, not including the first character of the line.
- $ Matches the end of a line, not including the last character or the line.

Marked Group

A section beginning with open parenthesis and ending with a closed parenthesis acts as a Marked Group. The string that matches the group pattern is preserved for later use.

- ( ) Used to group expressions and to capture a set of characters for use in a back-reference.

Shorthand Character Classes

Shorthand expressions describe a class of characters, for example, \d matches any numeric digit.

- \d Matches a numeric digit (0-9)

Repeaters

The repeater characters (*, +, ?, and {}) enable matching of a character, expression, or character class that is repeated.

- * Match the preceding character or expression from zero to unlimited times.
- [n] Match the preceding character or expression exactly n times.

Enable and Disable Inbound Calling Number Normalization Operations

A user assigned to the OCSS Configuration Editor role can enable or disable the Oracle® Communications Security Shield Cloud Service (Security Shield) inbound calling number normalization feature as needed. The default state is enabled.

Before You Begin

- Confirm that you are assigned to the OCSS Configuration Editor role.

Procedure
The following procedure enables or disables the inbound calling number normalization feature.

> **Note:**
>
> You can enable or disable inbound calling number normalization rules individually.

1. Access the **Settings** page and click **Number Normalization**.
2. On the Number Normalization page, click **State** and do one of the following:
    - Click Enabled. (Default)
    - Click Disabled.

Next Steps

- Add New Inbound Phone Number Normalization Rules

Add New Inbound Phone Number Normalization Rules

To specify how Oracle® Communications Security Shield Cloud Service (Security Shield) transposes phone numbers from a variety of formats into the E.164 format, you can create up to twenty-three rules for inbound phone number normalization in addition to the two default rules.

Before You Begin

- Confirm that you are assigned to the OCSS Configuration Editor role
- Enable and Disable Inbound Calling Number Normalization Operations

Procedure
Use the following procedure to add Number Normalization rules.

1. Access the **Settings** page and click **Number Normalization**.
2. On the Number Normalization page, click **Add Normalization Rule**.
3. In the Add Normalization Rule drawer, do the following:
    - Name—Enter up to 255 characters to create a unique name or description for the rule.
    - State—Set the state for the rule. Valid values: Enabled | Disabled.
    - Number Type—Set the geographic scope of the number you want normalized. When you select National, the dialog displays the Number Length and Digits to Prepend fields. When you select International, the dialog hides the Number Length field and Digits to Prepend fields. Valid values: National | International.
    - Number Prefix—Set the leading digits (including the + character) you want removed from the inbound calling number. The number of digits (including the + character) you set here must match the number you set in the Number of Leading Digits to Remove parameter. For example, if you enter the prefix +44 here, you must set the Number of Leading Digits to Remove parameter to 3.
    - Number Length—Set the rule for matching the number length. When you select Range, the dialog displays controls for setting the minimum and maximum number of digits. Valid values: Any | Exactly | Range.
    - Number of Leading Digits to Remove—Set the number of leading digits you want removed (including the + character). The number you set here, must match the

number of digits (including the + character) you entered in the Number Prefix parameter.

- Digits to Prepend—Set a choice for the number of digits to prepend. Valid values: None—Hides the digits entry field. | Country Code—Displays the "Select Country" field and drop-down list. | Other—Displays a blank field where you can enter 1-15 digits.
- Calling Number Pattern—Not directly configurable. As you configure the number normalization rule, Security Shield auto fills this field based on your input from the preceding parameters.
- Translation Pattern—Not directly configurable. As you configure the number normalization rule, Security Shield auto fills this field based on your input from the preceding parameters.

4. Do one of the following:
   - Click **Add** —Adds the rule to the table and closes the dialog.
   - Click **Add Another**—Adds the rule to the table, keeps the dialog displayed, and clears the settings so you can create another rule.

Edit an Inbound Calling Number Normalization Rule

A user assigned to the OCSS Configuration Editor role can edit an Oracle® Communications Security Shield Cloud Service (Security Shield) inbound calling number normalization rule. Security Shield updates the Calling Number Pattern and Translation Pattern as you edit the rule.

Before You Begin

- Confirm that you are assigned to the OCSS Configuration Editor role.

Procedure
Use the following procedure to edit Number Normalization rules.

1. Access the **Settings** page and click **Number Normalization**.
2. In the table on the Number Normalization page, locate the row that you want to edit.
3. Click the edit icon.

   Security Shield displays the Edit Number Normalization Rule dialog.
4. Edit as many Inbound Calling Number Normalization Configuration Parameters as needed.
5. Click **Save**.

Delete an Inbound Calling Number Normalization Rule

A user assigned to the OCSS Configuration Editor role can delete an Oracle® Communications Security Shield Cloud Service (Security Shield) inbound calling number normalization rule.

Before You Begin

- Confirm that you are assigned to the OCSS Configuration Editor role.

Procedure
Use the following procedure to delete Number Normalization rules.

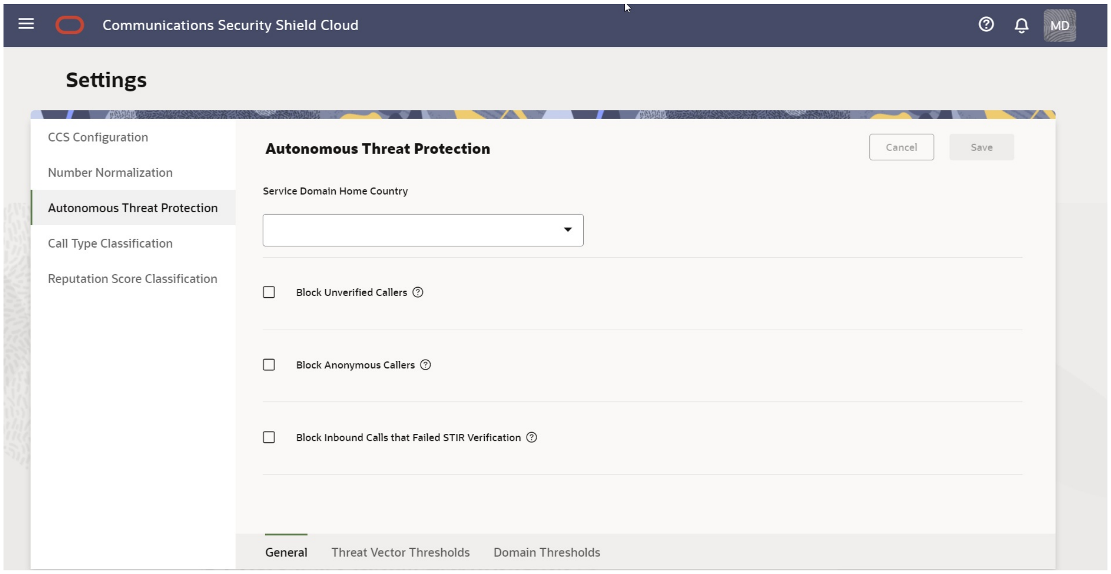
1. Access the **Settings** page and click **Number Normalization**.
2. In the table on the Number Normalization page, locate the row that you want to edit.
3. Click the delete icon and click **OK**.

   Security Shield displays a confirmation message.
4. Click **Delete**.

Autonomous Threat Protection Settings

After you install the Oracle® Communications Security Shield Cloud Service (Security Shield) service components, you can optionally change the default Security Shield settings that control and manage call activity passing through your Oracle Communications Session Border Controller (SBC). The default settings allow the Security Shield service to pass calls and perform services without further configuration or intervention. The default settings may or may not suit your business needs, so Oracle recommends that you consider the settings according to your needs and revisit them regularly. Adjusting the settings is a continuous process to engage in as your business evolves. You can make assessments and adjust the settings as needed, for example, to allow for marketing campaigns and daily call peaks.

The Settings page provides the entry point to the dialogs that you use to configure the General, Threat Vector Thresholds, and Domain Thresholds settings.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification
Autonomous Threat Protection
Cancel
Save
Service Domain Home Country
□ Block Unverified Callers
□ Block Anonymous Callers
□ Block Inbound Calls that Failed STIR Verification
General
Threat Vector Thresholds
Domain Thresholds

See the following topics for information about the types of Autonomous Threat Protection settings shown in the preceding screen capture.

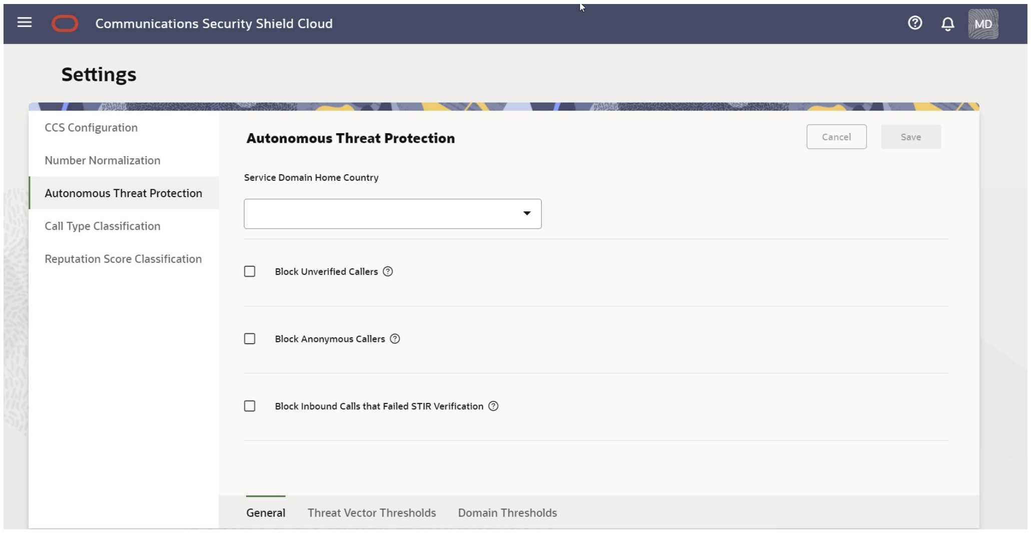
Autonomous Threat Protection General Settings

Threat Vector Thresholds

Domain Thresholds

Autonomous Threat Protection General Settings

On the Settings page, click General to display the autonomous threat protection settings that affect your deployment globally. Oracle recommends that you revisit these settings regularly because adjusting them is a continuous process as your business needs change. For example, you might need to adjust the settings to allow for marketing campaigns and daily call peaks.



Autonomous Threat Protection

Service Domain Home Country

□ Block Unverified Callers

□ Block Anonymous Callers

□ Block Inbound Calls that Failed STIR Verification

Service Domain Home Country—Your physical geographical location. The Security Shield verifies that a call uses the same country code as the home country, which defines all other calls as international. No default.

Block Unverified Callers—When enabled, the Security Shield blocks inbound, unverified callers. Default: Disabled.

Block Anonymous Callers—When enabled, the Security Shield blocks 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. Also, when the FROM header includes a phone number and PAI is either not present or shows a phone number and the Privacy header includes any of the privileged values, such as: "ïd", "user", or "header",Security Shield, blocks the call. Default: Disabled.

Block Inbound Calls that Failed STIR Validation—When enabled, Security Shield overrides the reputation score enforcement action configuration for a call that failed STIR verification at your SIP trunk provider or your Service Provider and blocks the call. When disabled, Security Shield uses the final reputation score, Access Control List, or Call Type enforcement action to determine the enforcement action for a call that failed STIR verification at your SIP trunk provider or your Service Provider. When a call fails STIR verification and the configured enforcement action for the reputation score is other than "Block" (for example: Continue), Security Shield applies the configured action and does not block the call. Default: Disabled.

> **Note:**
>
> The STIR validation indicator is received from the SIP Trunk provider or Communication Service Provider (CSP) in the INVITE. The STIR validation is not an action by Security Shield. The CSP checks for presence of the parameter, and based on the value, determines whether the STIR validation failed in the service provider network.

See Edit General Settings.

Edit General Settings

Provisioning the Oracle® Communications Security Shield Cloud Service (Security Shield) requires you to set the Service Domain Home Country to define which calls to consider as in-country. The other settings on the Settings tab are optional.

Procedure
Use the following procedure to set global settings for your call traffic.

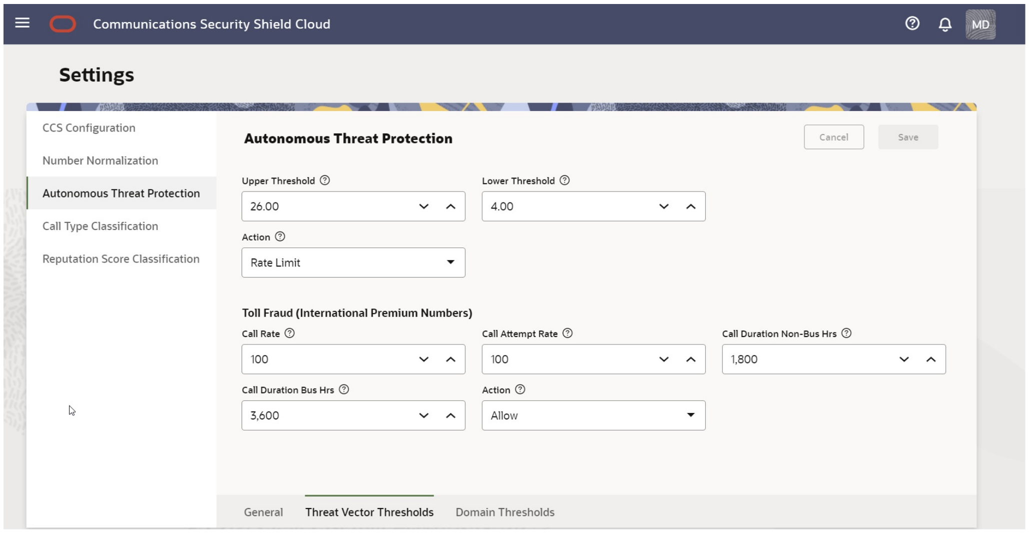
1. Access the **Settings** page, click **Autonomous Threat Protection**, and then **General**.
2. On the **Autonomous Threat Protection, General** page, do the following.

(Required) Service Domain Home Country	Select the home country from the drop-down list. Security Shield defines all other calls as foreign.
(Optional) Block Unverified Callers	Select to enable allowing callers that Security Shield cannot verify. Default: Deselected.
(Optional) Block Anonymous Callers	Select to enable allowing 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. Default: Deselected.
(Optional) Block Inbound Calls that Failed STIR Validation	Select to enable blocking calls that do not pass SITR validation, regardless of the configured reputation score action. Default: Deselected.

3. Click **Save**.

Threat Vector Thresholds

The Threat Vector Thresholds dialog on the Autonomous Threat Protection tab contains settings for managing risky call traffic and call flooding. Oracle sets the defaults for the thresholds, which you can change at any time with no reboot required. Oracle recommends that you revisit the Autonomous Threat Protection settings regularly because adjusting them is a continuous process as your business evolves. You can adjust the settings as needed, for example, to allow for marketing campaigns, daily call peaks, and other reasons for tightening or loosening control of call traffic volume.



Autonomous Threat Protection

Upper Threshold: 26.00

Lower Threshold: 4.00

Action: Rate Limit

Toll Fraud (International Premium Numbers)

Call Rate: 100

Call Attempt Rate: 100

Call Duration Non-Bus Hrs: 1,800

Call Duration Bus Hrs: 3,600

Action: Allow

Traffic Pumping—Sets upper and lower boundaries for the call attempt rate to prevent artificially high inbound call rates per interval of time.

- Call Attempt Rate for Business Hours
  - Upper Threshold—Set the number of call attempts per second at which you want the session border controller to recognize call flooding and start performing the configured action during business hours. Default: 25.00 Valid values: 1.00-100.00
  - Lower Threshold—Set the number of call attempts per second at which you want the session border controller to resume allowing all calls after a call flooding incident that occurred during business hours. Default: 20.00 Valid values: 1.00-100.00
- Call Attempt Rate for Non-Business Hours
  - Upper Threshold—Set the number of call attempts per second at which you want the session border controller to recognize call flooding and start performing the configured action during non-business hours. Default: 25.00 Valid values: 1.00-100.00
  - Lower Threshold—Set the number of call attempts per second at which you want the session border controller to resume allowing all calls after a call flooding incident that occurred during non-business hours. Default: 20.00 Valid values: 1.00-100.00
- Action—Set the action you want the session border controller to perform when Security Shield detects call flooding. Default: Continue. Valid values: Continue | Block | Rate Limit.

Toll Fraud (International Premium Numbers)—Helps the system to discover voice mail hijacking or PBX hacking.

- Call Rate—The number of active calls to international premium numbers that you want to allow. Default: 100. Valid values: 1-10,000.
- Call Attempt Rate—The number of call attempts to international premium numbers per session border controller per second that you want to allow. Default: 1000. Valid values: 1-100,000.

- Call Duration Non-Bus Hrs—The total call duration (in seconds) for all calls to premium rate services, toll free numbers, and international destinations per second during non-business hours. Default: 1,800. Valid values:1-1,000,000.
- Call Duration Bus Hrs—The total call duration (in seconds) for all calls to premium rate services, toll free numbers, and international destinations per second during business hours. Default: 3,600. Valid values:1-1,000,000.
- Action—The action to take when the Security Shield detects Toll Free Fraud. Default: Allow. Valid values: Allow | Block.

Enforcement Action Descriptions

The following enforcement actions apply to the preceding parameters

- Block—Terminates the calls to prevent them from traversing the session border controller.
- Continue—Lets call evaluation continue to the next stage even when Security Shield detects threats, anomalies, or incidents. No enforcement action is applied for the threat, anomaly, or incident until further processing of the reputation score indicates that the call is in a high-risk category. Security Shield then applies the enforcement action you configured for the risk category.
- Rate Limit—Drops calls randomly when the incoming call rate exceeds the configured call rate until the rate of calls no longer exceeds the configured rate.

See Edit Threat Vector Thresholds.

Edit Threat Vector Thresholds

Oracle provides the Oracle® Communications Security Shield Cloud Service (Security Shield) software with default threat vector settings so the system is ready to run the threat algorithms, detect potential threats, and perform protective actions without further input. If you want to change any of the defaults, you can reset them.

Procedure
The following procedure lists the defaults, ranges, and valid values that you can set according to the needs of your deployment. You do not need to restart the system after making changes, but you do need to save the changes.

You can set the following actions for Call Attempt Rate for Non Business Hours and Call Attempt Rate.

- Block—Terminates the calls to prevent them from traversing the session border controller.
- Continue—Lets call evaluation continue to the next stage even when Security Shield detects threats, anomalies, or incidents. No enforcement action is applied for the threat, anomaly, or incident until further processing of the reputation score indicates that the call is in a high-risk category. Security Shield then applies the enforcement action you configured for the risk category.
- Rate Limit—Drops calls randomly until the rate of calls traversing the session border controller matches the configured Call Attempt Rate Limit.

1. Access the Settings page, click **Autonomous Threat Protection** and then click **Threat Vector Thresholds**.
2. On the **Threat Vector Thresholds** page, do the following.

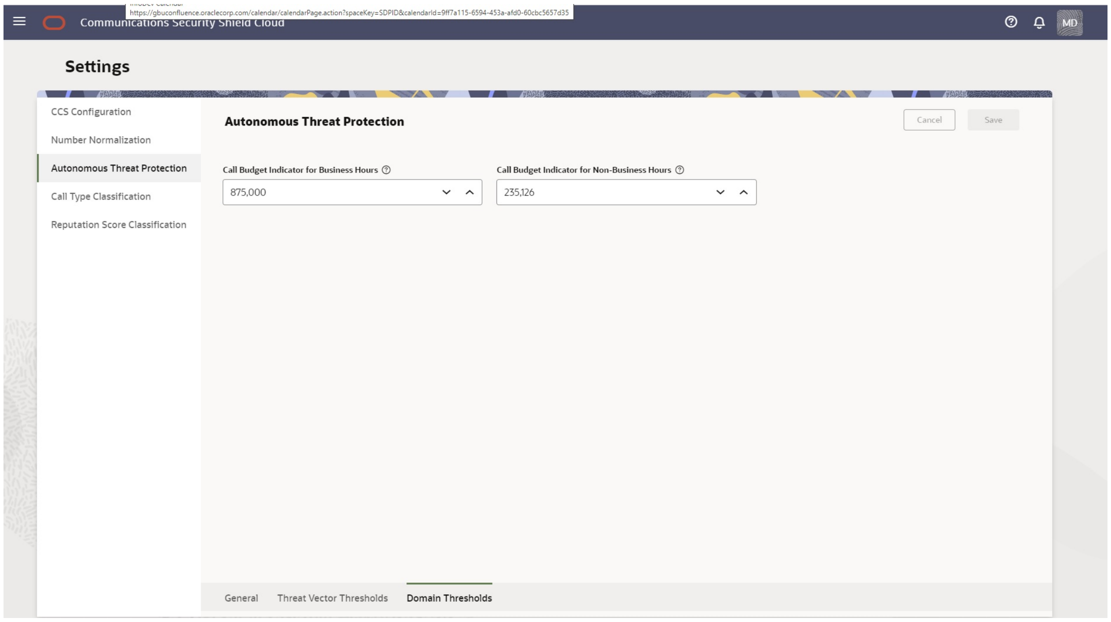
Traffic Pumping	• Call Attempt Rate for Business Hours – Upper Threshold—Set the number of call attempts per second at which you want the session border controller to recognize call flooding and start performing the configured action during business hours. Default: 25 calls per second. Valid values: 1.00-100.00 calls per second. – Lower Threshold—Set the number of call attempts per second at which you want the session border controller to resume allowing all calls after a call flooding incident that occurred during business hours. Default: 20 calls per second. Valid values: 1.00-100.00 calls per second. **Note:** The Lower threshold value for Traffic Pumping must be lower than Upper threshold for Traffic Pumping. • Call Attempt Rate for Non-Business Hours – Upper Threshold—Set the number of call attempts per time interval at which you want the SBC session border controller to recognize call flooding and start performing the configured action during non-business hours. Default: 25 calls per second. Valid values: 1.00-100.00 calls per second. – Lower Threshold—Set the number of call attempts per time interval at which you want the session border controller to resume allowing all calls after a call flooding incident that occurred during non-business hours. Default: 20 calls per second. Valid values: 1.00-100.00 calls per second. • Action—Set the action you want the session border controller to perform when Security Shield detects call flooding. Default: None. Valid values: Continue | Block | Rate Limit.
Toll Fraud (International Premium Numbers)	• Call Rate—Set the number of international calls per time interval that you want to allow. Default: 500. Valid values: 1-10,000. • Call Attempt Rate—Set the number of outbound calls per Session Border Controller per time interval that you want to allow. Default: 100. Valid values: 1-100,000. • Call Duration Non-Business Hrs—The total call duration (in seconds) for all calls to premium rate services, toll free numbers, and international destinations per time interval during non-business hours. Default: 3,600 seconds. Valid values: 1,000,000 seconds

- Call Duration Bus Hrs—The total call duration (in seconds) for all calls to premium rate service, toll free numbers, and international destinations per time interval during business hours. Default: 3,600 seconds. Valid values: 1-1,000,000 seconds.
- Call Cost—Set the threshold on the number so calls allowed to high risk (international) destinations. Default: 500. Valid values: 1-10,000.
- Action—Set the action that you want the session border controller to perform when Security Shield detects toll fraud. Default: Allow. Valid actions: Allow | Block.

3. Click **Save**.

Domain Thresholds

The Domain Thresholds dialog contains settings that inform the Oracle® Communications Security Shield Cloud Service (Security Shield) about how you want to manage risky call traffic within the Security Shield domain. Domain means all of the components and configurations used by, and affected by, the Security Shield. The Security Shield domain does not refer to, or equate to, the domain used for your Oracle Communications Session Border Controller, for example. Oracle recommends that you revisit these settings regularly because adjusting them is a continuous process as your business evolves. You can make assessments and adjust the settings as needed, for example, to allow for marketing campaigns and daily call peaks.


https://gbuconfluence.oraclecorp.com/calendar/calendarPage.action?spaceKey=SDPID&calendarId=9ff7a115-6594-453a-afd0-60cbc5657d35
Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification
Cancel
Save
General
Threat Vector Thresholds
Domain Thresholds

Autonomous Threat Protection

Call Budget Indicator for Business Hours: 875,000

Call Budget Indicator for Non-Business Hours: 235,126

Call Budget Indicator for Business Hours—The threshold for detecting unusual spikes to high-cost destinations during business hours. Default: 10,000. Range: 1-1,000,000.

Call Budget Indicator for Non-Business Hours—The threshold for detecting unusual spikes to high-cost destinations during non-business hours. Default: 1,000. Range: 1-1,000,000

See Edit Domain Thresholds.

Edit Domain Thresholds

The Oracle® Communications Security Shield Cloud Service (Security Shield) provides settings for your domain that help control unusual spikes to high-cost calling destinations. You can set thresholds for business hours and non-business hours.

Procedure
Use the following procedure to set call-budget thresholds according to the needs of your deployment.

1. On the **Settings** page, click **Autonomous Threat Protection**, and then click **Domain Thresholds**.
2. On the **Domain Thresholds** page, do the following.

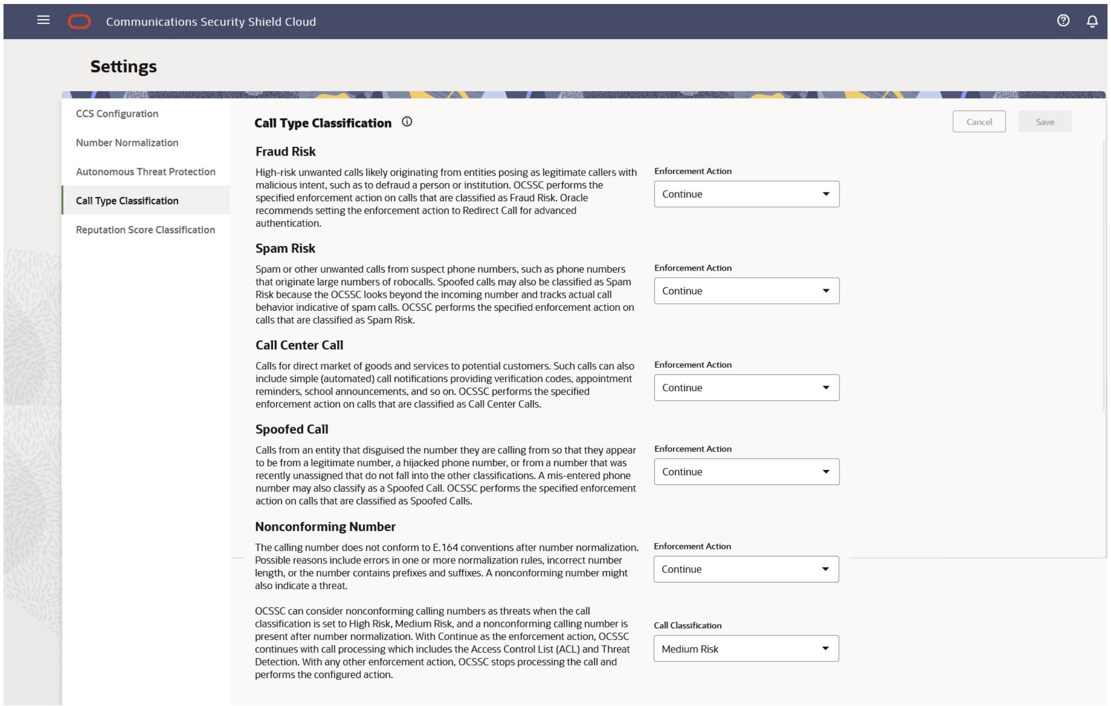
Call Budget Indicator for Business Hours	Set the threshold for detecting unusual spikes to high-cost destinations during business hours. Default: 10,000. Range: 1-1,000,000.
Call Budget Indicator for Non-Business Hours	Set the threshold for detecting unusual spikes to high-cost destinations during non-business hours. Default: 1,000. Range: 1-1,000,000.

3. Click **Save**.

Call Type Classifications

Certain incoming calls might represent low-value, no-value, or other unwanted calls to your business and you might want to get a more accurate understanding of such traffic so you can mitigate the subsequent unwanted effects on your call center. The Oracle® Communications Security Shield Cloud Service (Security Shield) Settings page displays a set of call type classifications and definitions for low-value or no-value calls, along with configurable enforcement actions. You can monitor the success of your enforcement actions on the Dashboard and then return to the Call Type Classifications page to change enforcement actions as needed.

The following screen capture shows the Call Type Classification page for Premium subscribers.


Communications Security Shield Cloud
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification
Cancel
Save

Call Type Classification ⓘ

Fraud Risk

High-risk unwanted calls likely originating from entities posing as legitimate callers with malicious intent, such as to defraud a person or institution. OCSSC performs the specified enforcement action on calls that are classified as Fraud Risk. Oracle recommends setting the enforcement action to Redirect Call for advanced authentication.

Enforcement Action: Continue

Spam Risk

Spam or other unwanted calls from suspect phone numbers, such as phone numbers that originate large numbers of robocalls. Spoofed calls may also be classified as Spam Risk because the OCSSC looks beyond the incoming number and tracks actual call behavior indicative of spam calls. OCSSC performs the specified enforcement action on calls that are classified as Spam Risk.

Enforcement Action: Continue

Call Center Call

Calls for direct market of goods and services to potential customers. Such calls can also include simple (automated) call notifications providing verification codes, appointment reminders, school announcements, and so on. OCSSC performs the specified enforcement action on calls that are classified as Call Center Calls.

Enforcement Action: Continue

Spoofed Call

Calls from an entity that disguised the number they are calling from so that they appear to be from a legitimate number, a hijacked phone number, or from a number that was recently unassigned that do not fall into the other classifications. A mis-entered phone number may also classify as a Spoofed Call. OCSSC performs the specified enforcement action on calls that are classified as Spoofed Calls.

Enforcement Action: Continue

Nonconforming Number

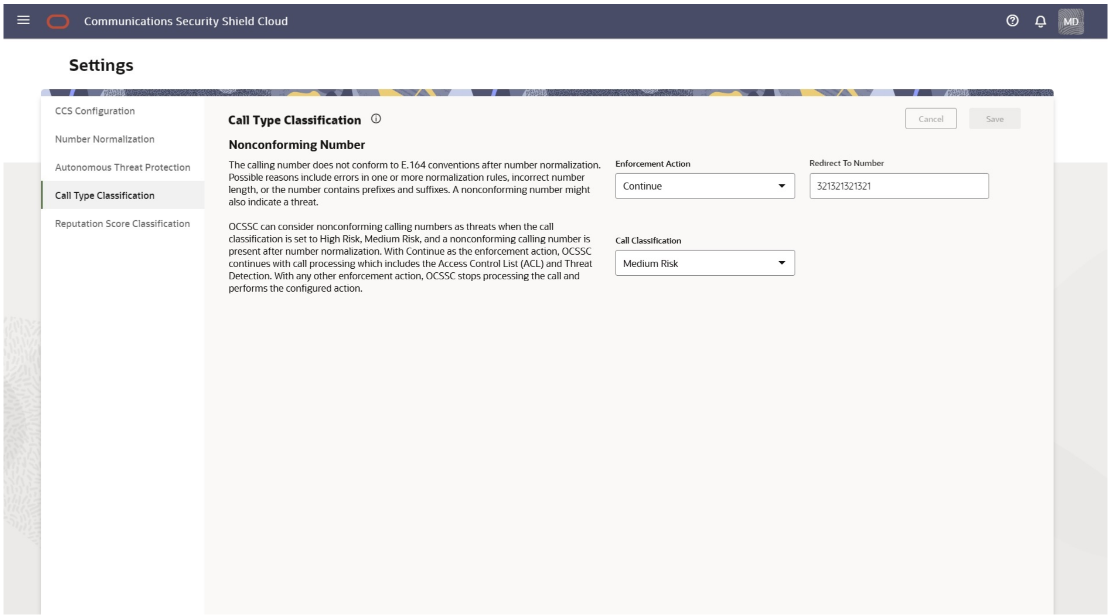
The calling number does not conform to E.164 conventions after number normalization. Possible reasons include errors in one or more normalization rules, incorrect number length, or the number contains prefixes and suffixes. A nonconforming number might also indicate a threat.

Enforcement Action: Continue

OCSSC can consider nonconforming calling numbers as threats when the call classification is set to High Risk, Medium Risk, and a nonconforming calling number is present after number normalization. With Continue as the enforcement action, OCSSC continues with call processing which includes the Access Control List (ACL) and Threat Detection. With any other enforcement action, OCSSC stops processing the call and performs the configured action.

Call Classification: Medium Risk

The following screen capture shows the Call Type Classification page for Standard subscribers.


Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification
Cancel
Save

Call Type Classification ⓘ

Nonconforming Number

The calling number does not conform to E.164 conventions after number normalization. Possible reasons include errors in one or more normalization rules, incorrect number length, or the number contains prefixes and suffixes. A nonconforming number might also indicate a threat.

Enforcement Action: Continue

Redirect To Number: 321321321321

OCSSC can consider nonconforming calling numbers as threats when the call classification is set to High Risk, Medium Risk, and a nonconforming calling number is present after number normalization. With Continue as the enforcement action, OCSSC continues with call processing which includes the Access Control List (ACL) and Threat Detection. With any other enforcement action, OCSSC stops processing the call and performs the configured action.

Call Classification: Medium Risk

Call Classifications and Descriptions

Security Shield determines the probability of the call to be a fraud risk, a spam risk, or a call center call based on the behavior of the caller by way of the phone number. The behavioral determination is separate from the call scoring that yields the reputation score. Occasionally the probability curve can label a call with a Good or Acceptable reputation score label, but with a call classification such as Fraud Risk or Spam Risk. Consider such instances as anomalies. Oracle works continuously to fine-tune the algorithms to avoid such anomalies. The Security Shield defines the call classifications, as follows.

- Fraud Risk (Premium subscribers)—High probability of a fraudulent call, likely originating from entities posing as legitimate callers with malicious intent, such as to defraud a person or institution. Security Shield performs the specified enforcement action on calls classified as Fraud Risk. Oracle recommends setting the enforcement action to Redirect Call for advance authentication.
- Spam Risk (Premium subscribers)—High probability of a robocall or other bad actor. Spoofed calls may also be classified as Spam Risk because Security Shield looks beyond the incoming number and tracks actual call behavior indicative of Spam calls. Security Shield performs the specified enforcement action on calls that are classified as Spam Risk.
- Call Center Call (Premium subscribers)—High probability of a call center call such as a telemarketer or call alerts. Such calls can also include simple (automated) call notifications providing verification codes, appointment reminders, school announcements, and so on. Security Shield performs the specified enforcement action on calls that are classified as Call Center Call.

> **Note:**
>
> Telemarketing calls can be a nuisance, but legal and useful. Although this category includes companies trying to sell services and goods, it also includes schools calling parents about a snow day or healthcare providers calling to make appointments for vaccinations. Use caution about selecting the Block enforcement action.

- Spoofed Call (Premium subscribers)—Calls from an entity that disguised the number they are calling from so that they appear to be from a legitimate number, a hijacked phone number, or from a number that was recently unassigned that do not fall into the other classifications. A mis-entered pone number may also classify as a Spoofed Call. Security Shield performs the specified enforcement action on calls that are classified as Spoofed Call.
- Nonconforming Number (Premium and Standard subscribers)—The calling number does not conform to E.164 conventions after number normalization. Possible reasons include errors in one or more normalization rules, incorrect number length, or the number contains prefixes and suffixes. A nonconforming number might also indicate a threat. Security Shield can also consider nonconforming calling numbers as threats when the call classification is set to High Risk or Medium Risk and a nonconforming number is present after number normalization. With Continue as the enforcement action, Security Shield continues with call processing which includes the Access Control List and Threat Detection. With any other enforcement action, Security Shield stops processing the call and performs the configured action.

Enforcement Actions

The Security Shield defines the enforcement actions, as follows:

- Block Call—Denies the call.
- Redirect Call—Redirects the call to the phone number that you specify.
- Continue—
  - If the Access Control List enforcement is set to Allow, Security Shield allows the call regardless of the enforcement action set for the reputation score.

- If the response code from the call look up is anything but Continue, Security Shield performs the specified action.
- If the response code from the call lockup is Continue, the call type is reported and no call enforcement is associated with this detection. Call enforcement depends on other threats detected or the reputation score enforcement and associated settings.

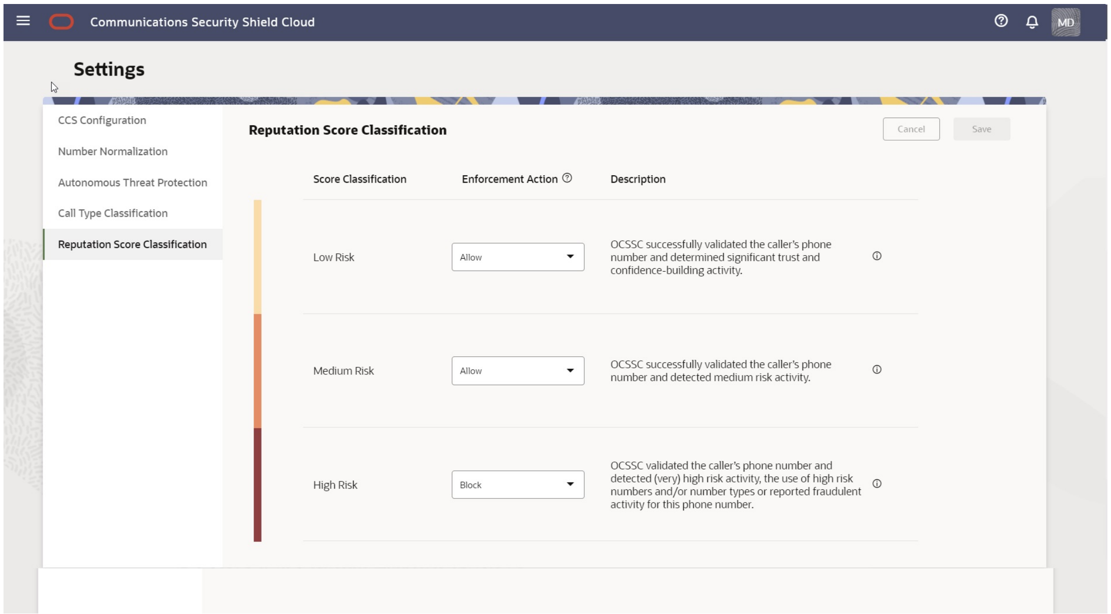
> **Note:**
>
> When there is a conflict between the Call Classification Type action and the Reputation Score Classification action, the Call Classification Type setting takes precedence.

Reputation Score Classification

From the Oracle® Communications Security Shield Cloud Service (Security Shield) Settings page, you can learn about reputation score classifications and set the enforcement action that you want the system to apply to each classification.

When you click **Reputation Score Classification**, Security Shield displays the reputation score call classifications, the possible enforcement actions, and descriptions. The iHelp explains the criteria for each classification.

The following screen capture shows an example of the Reputation Score Classification page.

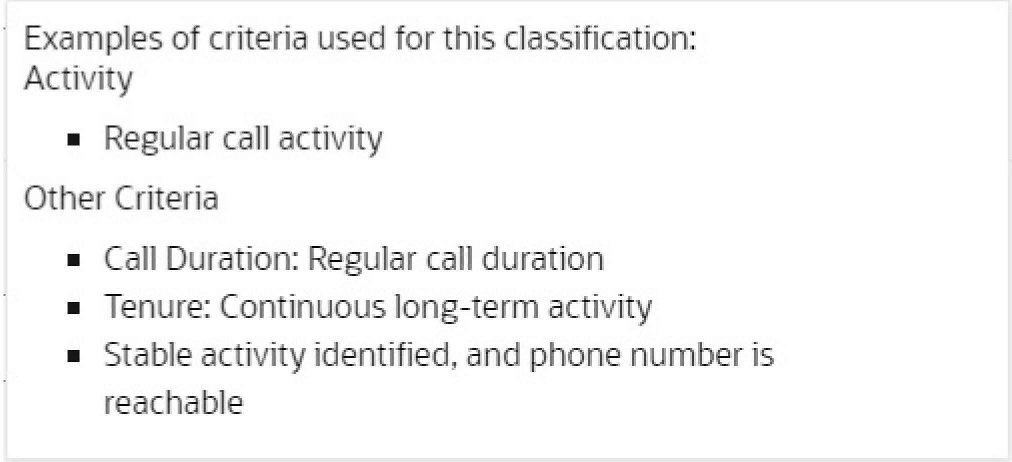

Communications Security Shield Cloud
MD
Settings
CCS Configuration
Number Normalization
Autonomous Threat Protection
Call Type Classification
Reputation Score Classification
Cancel
Save

Reputation Score Classification

Score Classification	Enforcement Action	Description
Low Risk	Allow	OCSSC successfully validated the caller's phone number and determined significant trust and confidence-building activity.
Medium Risk	Allow	OCSSC successfully validated the caller's phone number and detected medium risk activity.
High Risk	Block	OCSSC validated the caller's phone number and detected (very) high risk activity, the use of high risk numbers and/or number types or reported fraudulent activity for this phone number.

Classification Criteria

Low Risk classification criteria:



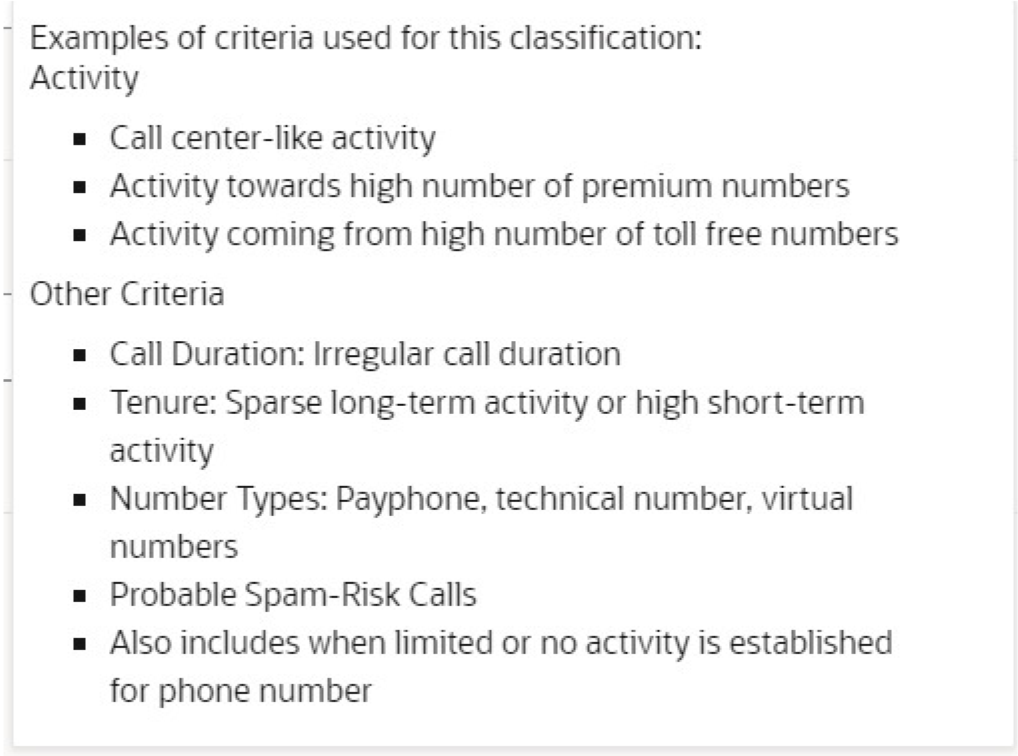
Examples of criteria used for this classification:
Activity

- Regular call activity

Other Criteria

- Call Duration: Regular call duration
- Tenure: Continuous long-term activity
- Stable activity identified, and phone number is reachable

Medium Risk classification criteria:



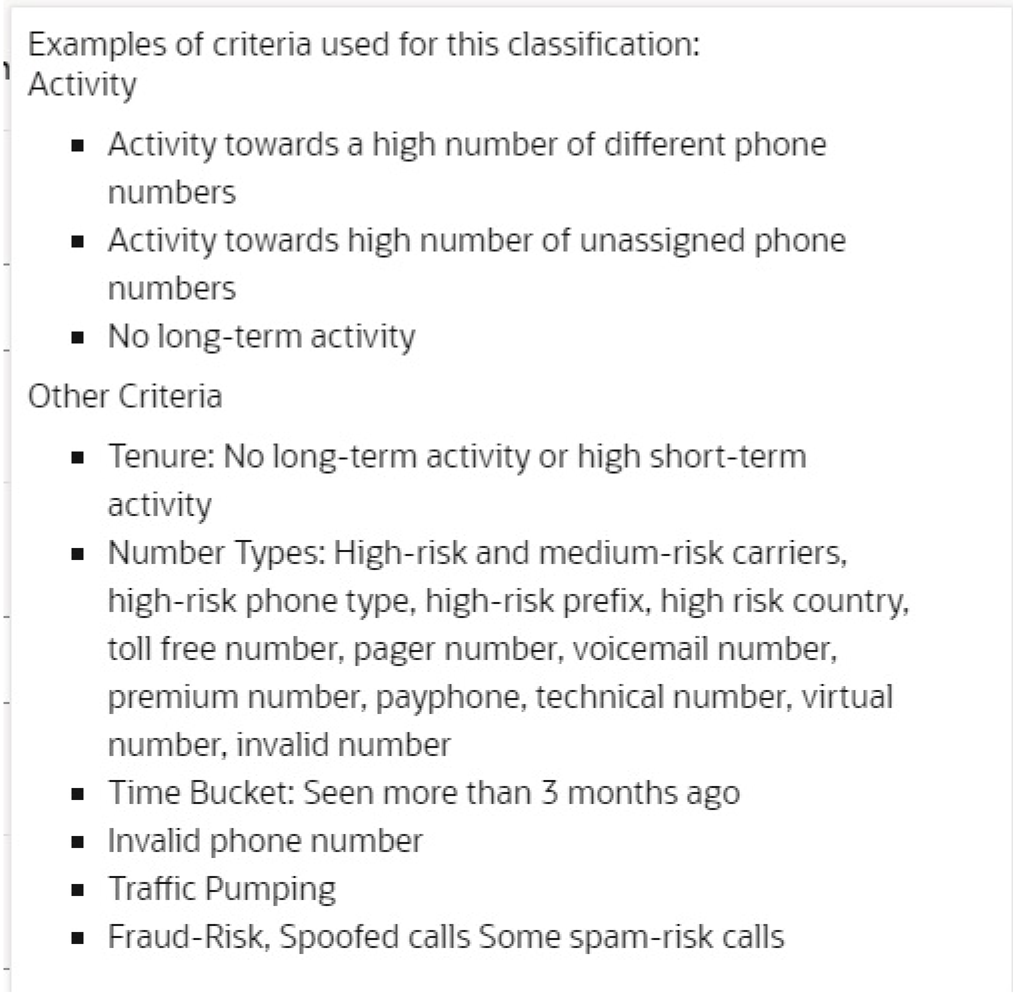
Examples of criteria used for this classification:
Activity

- Call center-like activity
- Activity towards high number of premium numbers
- Activity coming from high number of toll free numbers

Other Criteria

- Call Duration: Irregular call duration
- Tenure: Sparse long-term activity or high short-term activity
- Number Types: Payphone, technical number, virtual numbers
- Probable Spam-Risk Calls
- Also includes when limited or no activity is established for phone number

High Risk classification criteria:



Examples of criteria used for this classification:
Activity

- Activity towards a high number of different phone numbers
- Activity towards high number of unassigned phone numbers
- No long-term activity

Other Criteria

- Tenure: No long-term activity or high short-term activity
- Number Types: High-risk and medium-risk carriers, high-risk phone type, high-risk prefix, high risk country, toll free number, pager number, voicemail number, premium number, payphone, technical number, virtual number, invalid number
- Time Bucket: Seen more than 3 months ago
- Invalid phone number
- Traffic Pumping
- Fraud-Risk, Spoofed calls Some spam-risk calls

13

Security Shield Call Traffic Analytics

Oracle® Communications Security Shield Cloud Service (Security Shield) provides analytics that can help you investigate your inbound and outbound call traffic, as well as anomalies, suspicious behavior, and malicious traffic. You can access analytics through the Security Shield Dashboard.

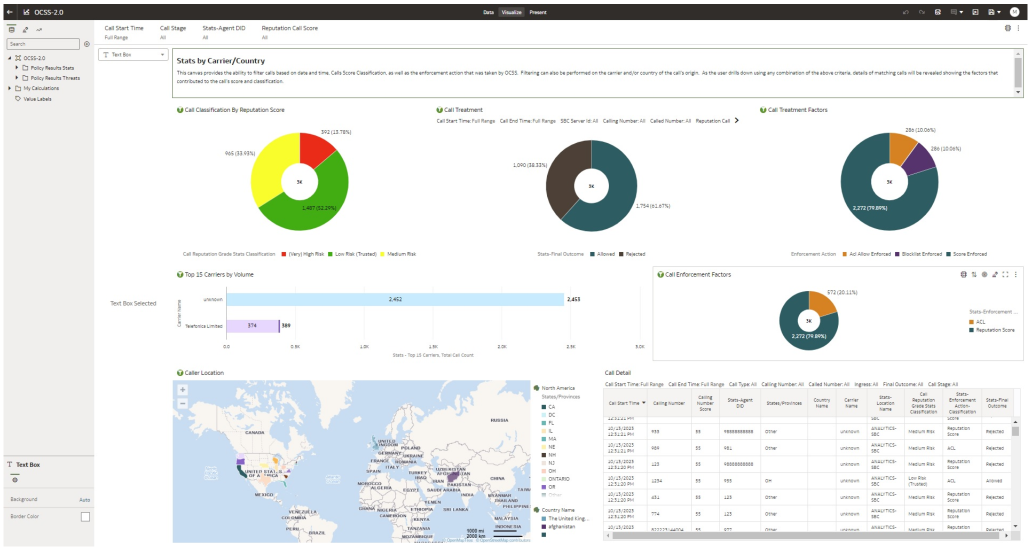
Topics:

Call Traffic Analytics Default Display

When you click the Analytic Reports button on the Oracle® Communications Security Shield Cloud Service (Security Shield) Dashboard, Security Shield opens the directory containing all analytics reports, called Projects. When you click the default Project, Security Shield displays the default set of canvases and opens to the Stats by Carrier/Country canvas.

> **Note:**
>
> Oracle periodically updates the default Project and versions its name. For example, OCSS-2.0 is newer than OCSS.

The following screen capture shows the Stats by Carrier/Country canvas as an example. Like all canvases, the display includes a combination of elements such as data attributes (located above the Call Classifications Reputation Score visualization), doughnut graphs, bar graphs, tables, and maps. The panel at the far left contains the attributes, elements, and formats privileged users can apply to the canvas. The panel between the far left panel and the canvas shows the attributes, elements, and formats used on the canvas in focus. Click the tabs at the bottom of the screen to see the other default canvases.



Stats by Carrier/Country

This canvas provides the ability to filter calls based on date and time, Calls Score Classification, as well as the enforcement action that was taken by OCSS. Filtering can also be performed on the carrier and/or country of the call's origin. As the user drills down using any combination of the above criteria, details of matching calls will be revealed showing the factors that contributed to the call's score and classification.

Call Detail

Call Start Time: Full Range Call End Time: Full Range Call Type: All Calling Number: All Called Number: All Ingress: All Final Outcome: All Call Stage: All

Call Start Time	Calling Number	Calling Number Score	Stats-Agent DID	States/Provinces	Country Name	Carrier Name	Stats-Location Name	Call Reputation Grade Stats Classification	Stats-Enforcement Action-Classification	Stats-Final Outcome
10/13/2023 12:31:21 PM	933	55	98888888888	Other		unknown	ANALYTICS-SBC	Medium Risk	Reputation Score	Rejected
10/13/2023 12:31:21 PM	989	55	981	Other		unknown	ANALYTICS-SBC	Medium Risk	ACL	Rejected
10/13/2023 12:31:20 PM	123	55	98888888888			unknown	ANALYTICS-SBC	Medium Risk	Reputation Score	Rejected
10/13/2023 12:31:20 PM	1234	55	955	OH		unknown	ANALYTICS-SBC	Low Risk (Trusted)	ACL	Allowed
10/13/2023 12:31:20 PM	431	55	123	Other		unknown	ANALYTICS-SBC	Medium Risk	Reputation Score	Rejected
10/13/2023 12:31:20 PM	774	55	123	Other		unknown	ANALYTICS-SBC	Medium Risk	Reputation Score	Rejected
10/13/2023	822223144004	55	977	Other		unknown	ANALYTICS-	Medium Risk	Reputation	Rejected

Note:

Oracle recommends that you use filters to limit the amount of data that is loaded for maximum 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.

The following table lists the tabs, data visualizations, and data attributes displayed on each of the default Security Shield canvases. For more information about each visualization, hover over the data elements in the visualizations and click the data attributes on the canvas. You can also use combinations of the attributes to see more or less data or different types of data. The visualizations on the canvas adjust to display details that correspond to the attributes you apply.

Note:

You can create customized versions of the default Projects with any of the attributes and formats listed in the left pane. Be sure to customize only a duplicate of the default Project; never the original.

Tabs	Descriptions
Stats by Carrier/Country	Filters calls based on Date, Time, Calls Score Classification, and the Enforcement action Security Shield applied. You can also filter on the Carrier and Country of origin.
Fraud Type by Carrier/Country	Filters calls based on Date, Time, Fraud Type, Score severity, and the Enforcement action Security Shield applied. You can also filter on the Carrier and Country of origin.
Country Statistics and Fraud Summary	Filters calls based on Country, Dialed Number, Date, Time, and Fraud Type.

Tabs	Descriptions
Carrier Statistics and Fraud Summary	Filters on Inbound Carrier, Dialed Number, Date, Time, and Fraud type.
Short Calls	Captures calls with durations under 10 seconds. Note: Although the duration does not trigger an enforcement action, you may find the data useful for identifying Account Takeover attempts, RoboCalls, and other Fraud attempts.
Neighbor Spoofing	Captures repeated calls from the same area code and prefix. Abnormal volumes of such traffic may indicate Neighbor Spoofing or an attempt to illicit a response to a call by spoofing a local phone number. Security Shield detects such patterns and dynamically adjusts the call score. You can configure Security Shield to block and redirect such calls.
Inbound Number Analysis	Filters calls based on Date, Time, Type of Fraud, Frequency of each Calling Number, Frequency of each Called Number, Carrier, and Country of origin.
Total Calls Table	Displays raw data related to every transaction processed through Security Shield. You can filter and sort the data by any data point in the table. You can export the data as a .CSV file for saving of further examination.
Call Stats	Displays a high-level, but detailed view of calls during the selected time period. The default view shows aggregate call totals and highlights inbound versus outbound, Session Border Controller location and score category distribution. Also shows the top ten FROM and To numbers and trend analysis of Call Enforcement, Call Rate, and Call Reputation Score.

Note:

Oracle recommends that you do not alter the default canvas. Instead, Duplicate the Default Analytics Project and alter the duplicate. After duplicating, be sure to Move a Security Shield Analytics Project Out of the OCSS Folder.

Change the Default Analytics Reports Display for Editing

The Oracle Analytics landing page defaults to the view-only mode, which does not allow editing. The OCSSAnalyticsEditor can edit the Call Statistics and the Call History reports, but must change the mode before editing is possible.

Procedure
The OCSSAnalyticsEditor must change the report mode (displayed in the URL) from the default "presentation" mode to the editing mode, called "full" mode. In this way, the OCSSAnalyticsEditor can edit the Call Statistics report and the Call History report, which are linked to the respective tiles on the Security Shield Dashboard.

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

Call Traffic Analytics Display Operations

All Oracle® Communications Security Shield Cloud Service (Security Shield) analytics canvases operate with the same behaviors and controls.

- When you click a particular part of the graphic in a visualization, the other visualizations on the canvas automatically adjust to filter on the same data point. For example, on the Stats by Carrier/Country canvas, suppose you click Medium Risk on the Call Classification by Reputation Score visualization. The data on all the other visualizations and tables changes to reflect data about only the Medium Risk calls.
- When you click an attribute at the top of the canvas, Security Shield displays a dialog for customizing the attribute. The parameters you set apply to all visualizations on the canvas.
- When you want to clear a filter in a visualization, click outside the visualization.
- When you want to clear all filters, move your cursor into the white space above the canvas. Security Shield displays a second hamburger menu. Click the menu and click either Clear All Selections or Remove All Filters.
- When you click a tab at the bottom of the canvas, Security Shield displays the corresponding set of visualizations.
- When no country name is identified for any call in the Call Detail visualization, the Caller Location map is inactive. If at least one call in the Call Detail visualization identifies a country, the map is active.
- When you alter filters or set a filter in a graphic the re-rendering may take time. The time is proportional to the amount of the data needed for the canvas. When a re-rendering takes too long, you may want to click Stop in navigation bar (to the right) and click again to re-initiate the rendering.
- When different calls contain numbers for which the first 30 digits are identical, OCSS Analytics considers them as the same number and not as unique numbers.

> **WARNING:**
>
> Regarding the following operations, Oracle strongly recommends that you never make changes to the default analytics Project. Always Duplicate the Default Analytics Project and move it out of the OCSS folder before making any changes.

- When you click the

  ⊕

  icon to the right of the last tab in the bottom row, Security Shield displays a blank canvas for creating one of your own design. If you do not see the **Add** icon, you are not assigned to the required OCSSAnalyticsEditor group. See "User Groups and Privileges" in the *Security Shield Installation and Maintenance Guide*.
- When you right-click the tabs at the bottom of the canvas, Security Shield displays controls for working with the canvas, such as Rename, Delete Canvas, Copy Canvas, Duplicate, Clear Canvas, and Canvas Properties.
- When you add or change data attributes and calculations on an existing canvas, Security Shield updates the visualizations and tables on the canvas. Oracle recommends that you use caution when adding or changing data attributes or calculations because the result may not be as intended due to the new combination of elements. You may need to fine-tune your selections to get the results you want, especially when you apply trellis columns and trellis rows to a visualization. In addition, the changes may result in longer load times for the canvas to display.
- When you try to add a format to a canvas that the data type does not support, the canvas displays "unavailable". For example, suppose you try to add Trellis Rows to a canvas for Call Classification by Reputation Score. The canvas displays "unavailable" in the gray column to the left of the canvas.

Policy Results Statistics Attributes

The following table lists and describes the attributes Oracle® Communications Security Shield Cloud Service (Security Shield) displays for creating custom Policy Results Statistics reports.

Table 13-1 Attributes for Use by Customers

Attributes	Description
Note: On-screen, an icon precedes each Policy Results Statistics attribute to identify the data type.	• # - The data type is numeric. • A - The data type is text. • Clock - The data type is time.
ACL Action	Indicates the Access Control List (ACL) action Security Shield applied.
Aggregated Time	Indicates the time at which the record was written to the database.

Table 13-1 (Cont.) Attributes for Use by Customers

Attributes	Description
Call End Time	The ending time of a call. The Call End time might not display when: • one of the parties has not terminated the call. • a network provider or a system in your organization's network has not canceled the call. • when Security Shield has not received the call termination update to Security Shield. • when the Session Border Controller has not sent the call termination update to Security Shield.
Call Frequency Limit Exceeded	Indicates that the number of successful calls made to a destination phone number exceeds the frequency threshold limit.
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 Security Shield 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. Alert reasons and names displayed in the notification message text include: – ACL Match—acl match – ACL Match and Allow—allowed – CLI Spoofing Suspected—invalid numbers (to=from) – Country Code (Destination) Does Not Exist—invalid country code – International Calls Fraud Suspected—fraud-like activity – Suspected Fraudulent Destination—high-risk destination – Suspected Toll Fraud—toll fraud-like activity – Suspected Traffic Pumping—traffic pumping-like activity

Table 13-1 (Cont.) Attributes for Use by Customers

Attributes	Description
Call Reputation Grade	The Call Reputation Grade based on the Reputation Score. The Reputation grades include: • Critical Risk • High Risk • Significant Risk • Severe Risk • Suspicious • Good • Acceptable • Unknown Note: When the call score is -1, unknown indicates the call is blocked by the customer's blocklist and Security Shield did not perform the reputation score calculation.
Call Stage	The stage of the call associated with the call record. For example: initiate, mid-call (where Security Shield provides an updated policy to the Session Border Controller) , terminate, and update (where the Session Border Controller sends additional information to Security Shield).
Call Start Time	The time at which the call started. Note: Call Start Time always displays a value.
Call Terminate State Trigger	Describes the trigger that lead the call to the determinant stage.
Call Termination Initiator	Describes the actor that terminated the call. For example, the caller, callee, Session Border Controller, Security Shield, or other.
Call Termination Reason	Describes the reason for call termination. For example: Canceled, Bye, noAnswer, errorResponse, or other.
Call Type	The call type in policy context. For example,International, Suspect, Toll Free, Premium Rate Service, and National.
Called Number	The called number from the TO header of the SIP call.
Called Number Score	The score assigned by Security Shield to the called number.
Calling Number	The calling number on record from the FROM header of the SIP call.
Calling Number Score	The score assigned by Security Shield to the calling number.
Carrier Name	The name of the telecom carrier of record. When Security Shield records do not contain carrier information for the calling number field, Security Shield leaves the field empty.
Country Name	The location of the Calling Number for inbound Calls.

Table 13-1 (Cont.) Attributes for Use by Customers

Attributes	Description
Enforcement Action	Comments about why the system applied a particular enforcement action. Comments include the following: • Suspected Toll Fraud • Suspected Traffic Pumping • Suspected Anonymous • FDCPA rule enforced • ACL Allow Enforced • ACL Exclude Enforced • Blocklist Enforced • CLI Verification Failed • Score Enforced
Enforcement Action Trigger	The trigger causing Security Shield to apply the final outcome. Triggers include: • Anonymous • Call center call • Enterprise lookup (for outbound calls) • Fraud risk • Managed list • Outbound call frequency limit • Reputation score • Spam risk • STIR TN validation unsuccessful • Spoofed call • Third party • Threats
Final Outcome	The enforcement action Security Shield applied, as determined by the Policy Decision Engine based on policy rules. Call actions include: • Allow • Exclude • Redirect • Reject • Rate limit
Ingress	A call direction parameter where "true" means the call is inbound and "false" means the call is outbound.

Table 13-1 (Cont.) Attributes for Use by Customers

Attributes	Description
Lookup Number	The phone number sent from the Session Border Controller to the Policy Decision Engine for enforcement determination. • Inbound calls—When the SIP INVITE includes a P-Asserted Identity (PAI) header, Security Shield sends the User portion of the PAI header in the Lookup Number field. When the SIP INVITE includes multiple PAI headers, Security Shield uses the phone number of the first tel PAI header. When no tel PAI header exists, Security Shield uses the User portion of the first SIP PAI header. • Outbound calls—Security Shield sends the User portion of the TO header.
PAI Display Name	The display name from the P-Asserted Identity header containing a name for the identified user.
PAI Host	The host domain portion of the P-Asserted Identity header.
PAI	The user portion of the P-Asserted-Identity header.
PDE Call End Time	The time at which the Policy Decision Engine initiates termination of a dangling call.
PDE Server ID	The unique ID of the Policy Decision Engine server. Used by Oracle personnel.
Phone Type	Indicates the type of device used to make the call. Devices include Fixed Line, Pager, Restricted or Premium, Toll Free, Voice Mail, and VoIP. Other results include Other, Null, and Unavailable.
Policies Applied Policy	The trigger causing Security Shield to apply the final outcome determined by the Policy Decision Engine. Triggers include: • Threats • Managed List • Reputation Score Action • Third Party • Enterprise Lookup
Policies Decision	Indicates whether or not the Fraud Detect Rule policy was applied. Values: True | False.
Policy Response Time	The number of milliseconds added to the call to send the policy request to the Policy Decision Engine, receive the policy response, and act on the response.
Policy Version	The version of the applied policy.
Realm	The realm for incoming and outgoing calls.
Reputation Call Score Count	The distribution for the configured time period for the reputation score by Call Stage, Call Start Time, Calling Number, Carrier Name, Country Name, Enforcement Action, and Reputation Call Score.

Table 13-1 (Cont.) Attributes for Use by Customers

Attributes	Description
Reputation Call Score	The reputation score for the call.
SBC Receive Time	The time at which the Policy Decision Engine receives the request from the Session Border Controller.
SBC Response Time	The time at which the Policy Decision Engine sends the response to the Session Border Controller.
SBC Server ID	The unique ID of the Session Border Controller server.
Service Provider	The name of the service provider.
Session ID	An encoded Base64 combination of the Call Timestamp, SBC ID, SIP Thread ID, Call ID, From tag, and Realm.
Stats ID Count	Indicates the number calls based on StatsId.

Table 13-2 Attributes Reserved for Oracle Personnel

Attribute	Descriptions
Aggregated Time	The time at which the record was written into the database. Used by the Security Shield Team for tracking and debugging.
GBUA Processed Timestamp	Used by the Security Shield team for tracking and debugging purposes.
Reputation Call Score Count	The count of the reputation score for a call.
Stats ID Count	The call count number based on Stats ID.

Policy Results Threats Attributes

The following table lists and describes the attributes Oracle® Communications Security Shield Cloud Service (Security Shield) displays for creating custom Policy Threats reports.

Table 13-3 Attributes for Use by Customers

Attributes	Description
Note: On-screen, an icon precedes each Policy Results Threat attribute to identify the data type.	• # - The data type is numeric. • A - The data type is text. • Clock - The data type is time.
Action Taken	The action Security Shield performed after detecting the threat.
Aggregated Time	Indicates the time at which the record was written to the database.

Table 13-3 (Cont.) Attributes for Use by Customers

Attributes	Description
Alert Reason	The text of the alert for a specific threat. Alerts include the following: • Suspicious No Value call:spam_risk • Suspicious No Value call:spoofed_call • Suspicious No Value call:call_center_call • Suspicious No Value call:fraud_risk • Invalid/CLI Spoofing • Malicious Behavior Detected • Suspected Traffic Pumping
Applied Policy	The name of the applied policy. For example, Fraud Detect Rule.
Call End Time	The ending time of a call. The Call End time might not display when: • one of the parties has not terminated the call. • a network provider or a system in your organization's network has not canceled the call. • when Security Shield has not received the call termination update to Security Shield. • when the Session Border Controller has not sent the call termination update to Security Shield.

Table 13-3 (Cont.) Attributes for Use by Customers

Attributes	Description
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 Security Shield 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. Alert reasons and names displayed in the notification message text include: – ACL Match—acl match – ACL Match and Allow—allowed – CLI Spoofing Suspected—invalid numbers (to=from) – Country Code (Destination) Does Not Exist—invalid country code – International Calls Fraud Suspected—fraud-like activity – Suspected Fraudulent Destination—high-risk destination – Suspected Toll Fraud—toll fraud-like activity – Suspected Traffic Pumping—traffic pumping-like activity
Call Frequency Limit Exceeded	Indicates that the number of successful calls made to a destination phone number exceeds the frequency threshold limit.

Table 13-3   (Cont.) Attributes for Use by Customers

Attributes	Description
Call Reputation Grade	The Call Reputation Grade based on the Reputation Score. The Reputation grades include: • Critical Risk • High Risk • Significant Risk • Severe Risk • Suspicious • Good • Acceptable • Unknown Note: When the call score is -1, unknown indicates the call is blocked by the customer's blocklist and Security Shield did not perform the reputation score calculation.
Call Score	The reputation score for the call.
Call Stage	The stage of the call associated with the call record. For example: initiate, mid-call, terminate, and update.
Call Start Time	The time at which the call started. Note: Call Start Time always displays a value.
Call Terminate State Trigger	Describes the trigger that lead the call to the determinant stage.
Call Termination Initiator	Describes the actor that terminated the call. For example, the caller, callee, Session Border Controller, Security Shield, or other.
Call Termination Reason	Describes the reason for call termination. For example: Canceled, Bye, noAnswer, errorResponse, or other.
Call Type	The call type in policy context. For example,International, Suspect, Toll Free, Premium Rate Service, and National.
Called Number	The called number from the TO header of the SIP call.
Called Number Score	The score assigned by Security Shield to the called number.
Calling Number	The calling number on record from the FROM header of the SIP call.
Calling Number Score	The score assigned by Security Shield to the called number.
Carrier Name	The name of the telecom carrier of record. If no data is provided, Security Shield cannot know or access this information. When Security Shield records contain no carrier for this calling number, the field displays empty.
Country Name	The location of the Calling Number for inbound Calls.

Table 13-3 (Cont.) Attributes for Use by Customers

Attributes	Description
Decision	The decision for whether or not the policy was applied. Values: True | False. Note: This field must be Boolean and cannot be null or missing.
Enforcement Action Comment	Comments about why Security Shield performed the particular action. Comments include the following: • Suspected Toll Fraud • Suspected Traffic Pumping • Suspected Anonymous • FDCPA rule enforced • ACL Allow Enforced • ACL Exclude Enforced • Blocklist Enforced • CLI Verification Failed • Score Enforced
Enforcement Action Trigger	The trigger causing Security Shield to apply the final outcome. Triggers include: • Anonymous • Call center call • Enterprise lookup (for outbound calls) • Fraud risk • Managed list • Outbound call frequency limit • Reputation score • Spam risk • STIR TN validation unsuccessful • Spoofed call • Third party • Threats
Final Outcome	The enforcement action Security Shield applied, as determined by the Policy Decision Engine based on policy rules. Call actions include: • Allow • Exclude • Redirect • Reject • Rate limit
Ingress	A call direction parameter. Values: True-indicates the call is inbound. False-indicates the call is outbound.

Table 13-3 (Cont.) Attributes for Use by Customers

Attributes	Description
Lookup Number	The phone number sent from the Session Border Controller to the Policy Decision Engine for enforcement determination. • Inbound calls—When the SIP INVITE includes a P-Asserted Identity (PAI) header, Security Shield sends the User portion of the PAI header in the Lookup Number field. When the SIP INVITE includes multiple PAI headers, Security Shield uses the phone number of the first tel PAI header. When no tel PAI header exists, Security Shield uses the User portion of the first SIP PAI header. • Outbound calls—Security Shield sends the User portion of the TO header.
PDE Call End Time	The time at which the Policy Decision Engine initiates termination of a dangling call.
PDE Server ID	The unique ID of the Policy Decision Engine server. Used by Oracle personnel.
Policy Response Time	The number of milliseconds added to the call to send the policy request to the Policy Decision Engine, receive the policy response, and act on the response.
Policy Version	The version of the applied policy.
Realm	The realm for incoming and outgoing calls.
SBC Receive Time	The time at which the Policy Decision Engine receives the request from the Session Border Controller.
SBC Receive Time	The time at which the Policy Decision Engine receives the request from the Session Border Controller.
SBC Response Time	The time at which the Policy Decision Engine sends the response to the Session Border Controller.
SBC Server ID	The unique ID of the Session Border Controller server.
Service Provider	Name of the Service Provider
Threat Count	The total number of calls received based on the Threat ID.
Threat ID	The unique ID of the particular threat associated with a call.
Threat Timestamp	The timestamp showing when Security Shielddetected the threat.

Table 13-3 (Cont.) Attributes for Use by Customers

Attributes	Description
Threat Vector Type	The name of the threat vector. Threat vectors include: • Call Center Call • Fraud Risk • Spam Risk • Spoofed Call • Toll Fraud • Traffic Pumping

Table 13-4 Attributes Reserved for Oracle Personnel

Attribute	Description
Aggregated Time	The time at which the record was written to the database. Used by Oracle employees for tracking and debugging.
GBUA Processed Timestamp	Used by the Security Shield team for tracking and debugging purposes.
PDE Server ID	The unique ID of the Policy Decision Engine server.
Policy Response Time	The number of milliseconds added to the call to send the policy request to the Policy Decision Engine, receive the policy response, and act on the response.

Calculation Attributes for Custom Call Reports

To refine the data displayed in an analytics canvas, you can apply the calculation attributes listed in the attributes pane. In the attributes pane, click **My Calculations** to see the list of parameters. The following topics lists and describe the calculation parameters.

Calculation Attributes for Use in Policy Results Stats Reports

Calculation Attributes for Use in Policy Results Threats Reports

> **Note:**
>
> For more information about creating your own calculations, see the Oracle Analytics Server and Oracle Business Intelligence Enterprise Edition at Oracle.com.

Calculation Attributes for Use in Policy Results Stats Reports

You can use the following Calculation Attributes in your Policy Results Stats reports.

Table 13-5 Policy Stats Reports Attributes

Attributes	Descriptions
Call Duration (HH:MM:SS)	Calculates the call duration between the Call Start Time and the Call End Time displayed in HH:MM:SS format. This field can be empty when there is no Call End Time received for a particular call.
Call Reputation Grade Stats Classification	Groups the call classifications from the reputation score into Critical Risk, Severe Risk, Significant Risk, High Risk, Suspicious, Acceptable, and Good for the visualization.
Latest Call Reputation Grade Stats Classification	The level of risk you want reported. Low, Medium, or High.
Max Duration	The maximum call duration of all the calls made from a particular calling number.
Reputation Score Average	Average of all the reputation scores received at that instant.
States/Provinces	The state or province you want reported.
Stats-Agent DID	The calling number from the FROM header in the SIP call.
Stats-Call Grade-Classification	Groups the call classifications based on the Reputation Call Score into the categories below.
Stats-Call Start Time-MM-DD-YYYY	The day, time, and year range for reporting.
Stats-Enforcement Action	Indicates why a particular action is applied.
Stats-Enforcement Action-Classification	Groups the call classifications based on the Enforcement Action Trigger into the categories below.
Stats-Final Outcome	The action taken against the call.
Stats-Location Name	The country source of the Calling Number for inbound Calls.
Stats-Number Group	Groups all the calls coming from a particular number.
Stats-Top15 Carriers	The top 15 carriers passing calls to your telecommunications network for the period.
Top 10 Called Number	Top 10 unique called numbers by based on number of occurrences in the TO header of the SIP call.
Top 10 Calling Number	Top 10 unique calling numbers based on number of occurrences in FROM header of the SIP call.
Total Call Count	

Note:

Do not use the parameters in the preceding list in Policy Results Threats reports. See Calculation Attributes for Use in Policy Results Threats Reports for the parameters you can use.

Calculation Attributes for Use in Policy Results Threats Reports

You can use the following Calculation Attributes in your Policy Results Threats Reports.

Table 13-6 Attributes for Policy Results Threats Reports

Attributes	Description
Call Reputation Grade Threats Classification	Groups the call classifications from the reputation score for threats into Critical Risk, Severe Risk, Significant Risk, High Risk, Suspicious, Acceptable, and Good visualization.
States/Provinces	The state or province you want reported.
Threats-Call Count	Total number of threats identified by Security Shield.
Threats-Enforcement Action-Comment	The comment about why a particular threat is detected.
Threats-Location Name	The source country of the Calling Number for which the threat is detected.
Threats-Number Group	Groups all the threats coming from a particular number.
Threats-Source Top 15 by Carrier	The top 15 carriers passing threats to your telecommunications network.
Total Threat Count	Indicates the number of unique threat-call records identified by Security Shield.
Threats-Threat Vector Proper	The type of threat detected .

Note:

Do not use the parameters in the preceding list in Policy Results Stats reports. See Calculation Attributes for Use in Policy Results Stats Reports for the parameters you can use.

Create Customized Analytics Projects

As a privileged user, you can create custom Oracle® Communications Security Shield Cloud Service (Security Shield) analytics projects to see the type of data you want in the format you want. You can create the projects with the attributes, calculations, data types, and formats that you choose.

Before You Begin

- Confirm that you are assigned to the OCSSAnalyticsEditor group. See "User Groups and Privileges" in the Security Shield Installation and Maintenance Guide.
- Create a Folder for Storing Analytics Projects other than in the OCSS folder.
- Duplicate the Default Analytics Project to start a new project. Oracle recommends that you always use the most recent Security Shield default Project. For example, OCSS 2.0 is newer than OCSS.

- Move a Security Shield Analytics Project Out of the OCSS Folder for safe keeping.
- See Policy Results Statistics Attributes, Policy Results Threats Attributes, and Calculation Attributes for Custom Call Reports for descriptions of the data types available for the analytics reports you want to create.

Procedure
In the following procedure, you drag and drop attributes from the Policy Results Stats, Policy Results Threats, or My Calculations lists from the left pane onto the canvas (the blank area in the center pane) or onto the (the blank area above the canvas) to create the analytics report. You can also use the formatting pane (displays between the visualization pane and the canvas after you click a parameter in the visualization pane) to further customize the report.

> **Note:**
>
> Do not combine attributes from Policy Result Stats and Policy Result Threats on the canvas. For example, do not put an attribute from Policy Results Stats into a Policy Results Threats visualization. Use only the attributes listed under the report type in use. The same rule applies when adding custom calculations.

1. On the Security Shield Dashboard, click **Analytics Reports**.

   Security Shield displays your projects on the Oracle Analytics page.

2. Click the duplicate project you made previously.

   Security Shield opens the project.

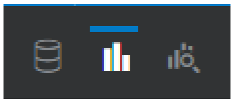
3. On the project, do as many of the following tasks as needed to prepare for creating a new project:

   Caution: Security Shield does not ask for confirmation before performing the following operations.

   - Clear a canvas completely—Right click the tab for any canvas you want to keep for customizing and click **Clear Canvas**. Security Shield removes all of the visualizations and keeps the canvas in the project.
   - Delete a canvas—Right click the tab (bottom row below the canvas) for any canvas you do not want and click **Delete Canvas**. Security Shield removes the canvas from the project.
   - Rename a canvas—Right click the tab for any canvas you want to keep and click **Rename**. Security Shield changes only the name of the canvas. The visualizations remain.
   - Remove a visualization from a canvas—Click a visualization, click the hamburger menu, and click **Delete Visualization**. Security Shield removes only the selected visualization.
   - Remove an attribute from a canvas—Hover over the attribute (located in the row above the canvas) you want to remove, click the arrow, and click **Delete**. Security Shield removes the attribute from the canvas.
   - Remove a format from the canvas—Select the visualization that uses the format, click the bulls eye icon, hover over the name of the format (the field changes from white to blue), and click the x to delete the format. Security Shield adjusts the visualization accordingly.

- Add a new canvas to the project—Click the + icon at the end of the bottom row of tabs to add a canvas. Security Shield adds a new, blank and unnamed canvas.

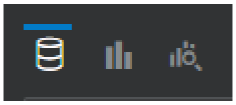
4. In the attributes pane, click the Format icon,

   scroll though the formats, and drag the format that you want onto the canvas.

   Security Shield adds the format to the pane between the visualizations pane and the canvas.

5. In the attributes pane, click the Data icon,

   and expand either Policy Results Stats or Policy Results Threats to see lists of the attributes you can add to the new visualization. Note: Call Stats is not available at this time.

6. Drag and drop the data elements you want onto the canvas.

   Security Shield begins building the new call-report visualization.

7. (Optional)—In the visualization pane, click **My Calculations** and double-click one or more of the calculation parameters.

   Security Shield adds the calculation type to the formatting pane and to the canvas.

8. (Optional)—In the formatting pane, use the layout and design controls to customize the visualization. Note: The controls vary according to the visualization type.

9. (Optional)—Above the formatting controls, click the ⊕ icon in the attributes bar that runs across the top of the canvas to see lists of attributes you can apply and do the following:

   - Expand the list according the type of visualization you are creating (Policy Results Stats or Policy Results Threats).
   - Double-click the element you want to use.
   - Configure the attribute and click outside of the configuration dialog to add it to the attributes bar.
   - (Optional)—Select and configure more attributes.

10. Click **Save**.

    Security Shield saves the new project.

> **Caution:**
>
> Do not keep your custom or modified analytics projects in the OCSS folder. When Oracle upgrades Security Shield, the process may overwrite the default canvas and will remove all canvases you added or modified in the OCSS folder. Oracle strongly recommends that when you create a custom analytics canvas or modify the default analytics canvas, you do so in a different folder. Oracle also recommends saving a local copy of all your analytics canvases. Use the export function, which creates a .dva file you can save locally. In this way, your canvases will be available for use in disaster recovery, roll-back, and upgrade scenarios. See Move a Security Shield Analytics Project Out of the OCSS Folder.

- For important information about saving custom analytics reports, see Save Analytics Projects .

Security Shield Analytics Export

Sometimes you might want to save or further examine information from the Oracle® Communications Security Shield Cloud Service (Security Shield) analytics canvas or share it with other trusted parties. You might also want to capture the same types of information on another of your other Security Shield tenancies. To accomplish those goals, you can export analytics data, graphs, and canvases to save and use as needed.

You can export the following from a canvas:

- Data from a single report displayed on the canvas
- The whole canvas
- A graphical image of a single report or the whole canvas

The export functionality provides several formats for the output.

- When you want to export data, choose the .csv format. Security Shield delivers the data in an Excel spreadsheet, which you can view and save immediately.

> **Note:**
>
> Security Shield can export approximately one million entries in a spreadsheet.

- When you want to export a canvas to save for backup or possibly a roll back, choose the Package .dva format. Security Shield delivers the canvas in a .dva file that you can save and upload when needed.
- When you want to export a graphical image of a canvas or report, choose the PowerPoint, Acrobat, or Image format. Security Shield delivers the file in the selected format, which you can view and save immediately.

Export Analytics Data from Security Shield

When you want to keep or further examine data from the Oracle® Communications Security Shield Cloud Service (Security Shield) analytics reports, you can export the data to a .csv file to save locally.

Before You Begin

- You must be assigned to the OCSSAnalyticsUser role to perform the following procedure.

Procedure
Use the following procedure for each report on the canvas from which you want to export data. Security Shield does not export data from multiple reports at the same time. When you click a report, Security Shield puts a frame around it to indicate it is the active one.

> **Note:**
>
> Security Shield can export approximately one million records in a spreadsheet.

1. Access the Security Shield Dashboard and click **Analytics Reports**.
2. On the **Oracle Analytics** page, click the canvas that contains the report you want to export.
3. On the canvas, click the tab at the bottom of the page with the **name of the canvas** you want to view.
4. On the canvas, click the report you want to export.
5. Click the **Export** icon at the right end of the page banner, and click **File**.
6. In the **File** dialog, for **Format**, select **Data .csv**.
7. Click **Save**.

   Security Shield delivers an Excel file to your screen.

Export an Analytics Canvas from Security Shield

You can save an Security Shield analytics canvas locally by exporting and saving it to a local folder.

Before You Begin

- You must be assigned to the OCSSAnalyticsUser role to perform the following procedure.

Procedure
Use the following procedure for each canvas you want to export. Security Shield does not export multiple canvases at the same time.

1. Access the Security Shield Dashboard, and click **Analytics Reports**.
2. On the **Oracle Analytics** page, click the canvas that you want to export.
3. Click the **Export** icon at the right end of the page banner, and click **File**.

4. In the File dialog, do the following:
   - Name—(Optional) Re-name the canvas.
   - Format—Select **Package (dva)**.
   - Include Data—Oracle recommends that you do not enable this option.
   - Include Connection Credentials—Oracle recommends that you do not enable this option.
   - Include Permissions—Oracle recommends that you do not enable this option.
   - Protect Password—(Optional) Protect the .dva package file with a password.
5. Click **Save**, and **Yes**.

   Security Shield exports the file to your screen.
6. Save the file locally for future use.

Export an Analytics Graph from Security Shield

When you want to keep or further examine Oracle® Communications Security Shield Cloud Service (Security Shield) analytics graphs, you can export the graphs as Image, PDF, or PowerPoint files that you can save locally.

Before You Begin

- You must be assigned to the OCSSAnalyticsUser role to perform the following procedure.

Procedure
Use the following procedure for each report on the canvas that you want to export as a graphic. Security Shield does not export multiple reports at the same time. When you click a report, Security Shield puts a frame around it to indicate it is the active one.

1. Access the Security Shield Dashboard, and click **Analytics Reports**.
2. On the **Oracle Analytics** page, click the canvas that contains the report you want to export.
3. On the canvas, click the report you want to export as a graphic.
4. Click the **Export** icon at the right end of the page banner, and click **File**.
5. In the **File** dialog, do the following:
   - Name—(Optional) Change the name of the file.
   - Format—Select Acrobat (.pdf), Image (.png), or PowerPoint (.pptx).
   - Include—Select which part of the canvas you want to export. The choices vary per Format type.
   - Size—Select the size you want for the output. Size displays only for Acrobat (.pdf) and PowerPoint (.pptx).
   - Orientation—Select the orientation for the output. Orientation displays only for Acrobat (.pdf) and PowerPoint (.pptx).
6. Click **Save**.

   Security Shield delivers the file to your screen.

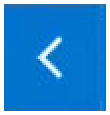
Update Custom Analytics Canvases

Some Oracle® Communications Security Shield Cloud Service (Security Shield) updates contain new data points that you can add to your existing custom analytics canvases. For example, My Calculations, Policy Results Statistics, or Policy Results Threats might contain new data points. See the What's New document to learn about any new data points.

Procedure
To add a new data point to an existing analytics canvas, you open the canvas and drag and drop the new data point onto the canvas from the list in the navigation pane.

1. On the Security Shield Dashboard, click **Analytics Reports**.
2. Click the **Back** button at the left end of the page banner.

   Back button.

3. On the Oracle Analytics home page, click the action menu at the left end of the page banner to display the navigation pane and click **Catalog**.

   Action menu.

4. On the Catalog page, click **Shared Folders** and then the folder where the canvas is located.
5. Open the canvas you want to update and drag and drop the new data point from the My Calculations, Policy Results Statistics, or Policy Results Threats lists onto the canvas.

Save Analytics Projects

When Oracle upgrades Security Shield, the process may overwrite the default project and will remove all other projects in the OCSS folder. Oracle strongly recommends removing all projects you want to keep from the OCSS folder and saving them elsewhere. You may want to keep local copies, as well. In this way, your projects will be available for use in disaster recovery, roll-back, and upgrade scenarios.

Use the following tasks as needed to save your Security Shield analytics canvases.

- Create a Folder for Storing Analytics Projects—Applies when you want to save your analytics canvases in a folder other than the OCSS folder.
- Duplicate the Default Analytics Project —Applies when you want to preserve or modify the default canvas.
- Move a Security Shield Analytics Project Out of the OCSS Folder—Applies to all analytics reports you want to preserve for future use.
- Export an Analytics Canvas from Security Shield—Applies to all analytics reports that you want to save locally.

> **Note:**
>
> When you re-import a locally saved canvas into a newer version of Security Shield, the canvas retains the look and functionality of the release of origin.

Duplicate the Default Analytics Project

To preserve the default Oracle® Communications Security Shield Cloud Service (Security Shield) analytics project, duplicate it and move it out of the OCSS folder. You can also use the following procedure to duplicate any of your custom analytics reports.

Before You Begin

- Create a Folder for Storing Analytics Projects

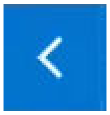
Procedure
Oracle periodically updates the default Project and versions its name. For example, OCSS-2.0 is newer than OCSS. Use the most recent default Project.

After you perform the following procedure be sure to save the duplicate in a folder other than the OCSS default folder because the software upgrade process may overwrite the default projects and will remove any other projects in the default folder.

> **Note:**
>
> Oracle recommends that you never directly modify a default project. Create a duplicate and modify the duplicate.

1. On the Security Shield Dashboard, click **Analytics Reports**.
2. Click the **Back** button at the left end of the page banner.

   Back button.

3. On the Oracle Analytics home page, click the action menu at the left end of the page banner to display the navigation pane and click **Catalog**.

   Action menu.

4. On the Catalog page, click **Shared Folders** and then click the **OCSS** folder.
5. On the project that you want to duplicate, click the action menu in the lower right hand corner and click **Duplicate**.

   The system displays another representation of the original report image and adds the word "Copy" to the name.

6. Rename the duplicate project with a unique name.
   - Hover over the report.

- Click the action menu.
- Click **Rename**.
- Enter the new name in the Name field. For example, Total Calls Backup.
- Click **OK**.

7. Repeat the process for each report you want to duplicate.

Next Steps

- Move a Security Shield Analytics Project Out of the OCSS Folder

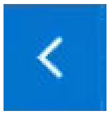
Create a Folder for Storing Analytics Projects

Before you create a new Oracle® Communications Security Shield Cloud Service (Security Shield) project or move an existing project out of the default OCSS folder, you need a destination folder.

Procedure
In the following procedure, you use the action menu on the default canvas to create a new folder.

1. On the Security Shield Dashboard, click **Analytics Reports**.
2. On the OCSS page, click the **Back** arrow at the left end of the page banner.

   Back button.

3. On the Oracle Analytics page, click the action menu at the left end of the page banner to display the navigation pane, and click **Catalog**.

   Action menu.

4. On the Catalog page, click **Shared Folders**.
5. On the Catalog page, click the actions menu in the upper right hand end of the banner and click **Create Folder**.
6. In the New Folder dialog, enter the name of the new folder (For example, My Custom Reports), and click **Create**.

   The system adds the new folder to the OCSS folder in Shared Folders.

7. Do one of the following:
   - Keep the new folder in Shared Folders, if you want to allow others access the new folder.
   - Move the new folder to My Folders, if you want to keep access to the new folder private.

Next Steps

- Move a Security Shield Analytics Project Out of the OCSS Folder into your new folder.

Move a Security Shield Analytics Project Out of the OCSS Folder

If the OCSS folder contains any projects you created or customized, Oracle strongly recommends moving them to a different folder because the upgrade process may overwrite the default project and will remove any other projects in the OCSS folder. Move projects to another folder if you want to preserve them.

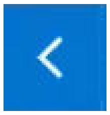
Before You Begin

- Create a Folder for Storing Analytics Projects.

Procedure
To move your analytics projects for safe keeping, access the OCSS folder and move them to the folder of your choice.

1. On the Security Shield Dashboard, click **Analytics Reports**.
2. Click the **Back** button at the left end of the page banner.

   Back button.

3. On the Oracle Analytics page, click the actions menu at the left end of the page banner to display the navigation pane and click **Catalog**.

   Action menu.

4. On the Catalog page, click **Shared Folders** and then the **OCSS** folder.
5. In the OCSS folder, select a project, click the action menu on the project, and click **Move to...**.
6. In the Move <Report Name> dialog, select the destination folder that you want. For example, Shared Folders or one that you created for storing reports, and click **Move**.
7. Move each report that you want to preserve to a destination folder other than OCSS.

Clear a Filter on an Analytics Visualization

After you filter data in a visualization or table in an analytics canvas by clicking a particular data point, you can clear the filter to return the visualization to its previous state.

Procedure

- In the visualization, click in the white space.

  Security Shield returns the visualization to its previous state.

A

Reference Information

The following topics provide reference information about the Oracle® Communications Security Shield Cloud Service (Security Shield).

- Security Shield Acronyms
- Security Shield Phone Number Format Requirements
- P-OCSS-Call-Info Header Element Descriptions
- P-OCSS-Call-Info Codes, Types, and Values

Security Shield Acronyms

Documentation for the Oracle® Communications Security Shield Cloud Service (Security Shield) uses the following acronyms.

ACLI	Acme Command Line Interface—The command line interface you can use for configuring the Oracle Communications Session Border Controller.
API	Application Programming Interface—An interface or common protocol used between parts of a computer program. Used to ease implementing and maintaining software.
CCS	Cloud Communication Service—The bi-directional Security Shield communication service between on-premises devices and the Oracle Cloud Infrastructure.
CLI	Calling Line Identity—A method of identifying the origin of and inbound call.
HA	High Availability—A method of pairing devices to ensure that one is always active.
IAM	Identity and Access Management—Ensures that the right people and job roles can access applications, data and digital assets.
IVR	Interactive Voice Response—An automated telephone system used to engage callers with prompts that provide actions and information without intervention from live agents.
LAN	Local Area Network—In the Security Shield, the LAN is the internal connection to the Policy Decision Engine.
OCI	Oracle Cloud Infrastructure—Oracle's cloud services platform where you can build and run a wide range of applications and services in a high availability, hosted environment.
PEP	Policy Enforcement Point—A session border controller, for example, that applies the actions that you specify to calls.
PSTN	Public Switched Telephone Network—A collection of interconnected, traditional circuit-switched telephone networks for voice communications.

REST	Representational State Transfer—When a client requests a resource by way of a REST API, the server sends the resource back in its current state in a standardized representation.
SaaS	Software as a Service—A distribution method, where a third-party hosts your software and makes it available over the Internet.
SBC	Session Border Controller—A device that you deploy on the border of your network to protect SIP-based Voice over Internet Protocol operations.
WAN	Wide Area Network—In the Security Shield, WAN is the external connection to the Oracle Cloud Infrastructure.