

**Oracle® Communications Fraud Monitor**

User's Guide

Release 4.1

**E99947-01**

November 2018

Oracle Communications Fraud Monitor User's Guide, Release 4.1

E99947-01

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

<b>Preface</b> .....	v
Audience .....	v
Downloading Oracle Communications Documentation .....	v
Documentation Accessibility .....	v
Document Revision History .....	v
<b>1 Overview of Fraud Monitor</b>	
<b>About Fraud Monitor</b> .....	1-1
<b>Logging In to Fraud Monitor</b> .....	1-1
<b>About Using the Fraud Monitor User Interface</b> .....	1-2
Overview Page .....	1-2
Viewing the Status for the Last Hour .....	1-3
Viewing the Latest Incidents .....	1-3
Viewing the Highest Scoring Users .....	1-4
How it Works .....	1-4
Incidents Page .....	1-4
Details Page .....	1-5
Performing a User Search .....	1-6
Deleting User-Specific Records .....	1-6
Viewing Score Information .....	1-6
Viewing Metric Information .....	1-6
User Menu .....	1-6
Editing the User Profile .....	1-7
Viewing System Information .....	1-7
Viewing License Information .....	1-7
Logging Out .....	1-7
Settings Page .....	1-7
<b>2 About Detecting Fraud</b>	
<b>How Fraud Monitor Detects Fraud</b> .....	2-1
<b>About Fraud Scenarios</b> .....	2-1
PBX Fraud .....	2-1
International Revenue Share Fraud .....	2-2
<b>About Fraud Detection Rules</b> .....	2-2
Traffic Profile .....	2-2

Blacklist and Whitelist Entries .....	2-2
Destination-Based Traffic Spikes .....	2-3

### **3 Installing Fraud Monitor**

Hardware Requirements .....	3-1
Installing Fraud Monitor .....	3-1

### **4 Configuring Fraud Monitor**

About Configuring Fraud Detection Rules.....	4-1
Configuring Rules.....	4-1
Setting Up Email Notifications.....	4-3
Adjusting the Notification Levels.....	4-3
Specifying Blacklist .....	4-4
Specifying Whitelist .....	4-4
Specifying Ratelimit List .....	4-4
Adding a Ratelimit User .....	4-5
Configuring Ratelimit.....	4-6
Specifying Redirect List.....	4-6
Adding a Redirect User.....	4-7
Configuring Redirect .....	4-8
Configuring Mediation Engine .....	4-8
Managing Users .....	4-9
Configuring Import/Export .....	4-10
Configuring Automatic List .....	4-11

## **Glossary**

---

---

# Preface

This guide describes how to install, configure, and use Oracle Communications Fraud Monitor.

The Oracle Communications Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Fraud Monitor
- Control Plane Monitor

## Audience

This guide is intended for system administrators, network administrators, and network operations team who use Oracle Communications Fraud Monitor to monitor calls and detect fraud.

## Downloading Oracle Communications Documentation

Oracle Communications Session Monitor documentation and additional Oracle documentation is available from the Oracle Help Center Web Site:

<http://docs.oracle.com>

## 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>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Document Revision History

The following table lists the revision history for this document:

<b>Version</b>	<b>Date</b>	<b>Description</b>
E99947-01	November 2018	Initial release.

---

---

# Overview of Fraud Monitor

This chapter provides an overview of Oracle Communications Fraud Monitor.

## About Fraud Monitor

The Session Monitor architecture consists of the Probe layer, Mediation Engine layer, and the Aggregation Engine layer (see the discussion about Session Monitor architecture in *Session Monitor Installation Guide* for information about the functions performed in each layer).

Fraud Monitor runs on the Aggregation Engine (AE) machine, but relies on the data provided by the Mediation Engines (MEs) to detect fraud. For each established call, the ME that has correlated the call, sends a notification to the AE, when the call is established, then one notification every few minutes and finally a notification at the end of the call. This allows Fraud Monitor to be aware of the real-time state of all the calls in the system and use this state to apply the different behavioral rules.

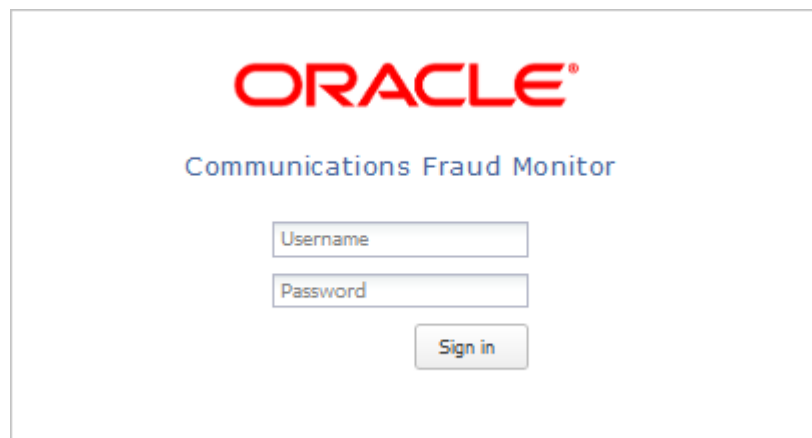
## Logging In to Fraud Monitor

The Login page allows you to access Fraud Monitor. Enter your user name and password into the indicated fields, then click **Sign in** to proceed to the application.

[Figure 1-1](#) shows the Fraud Monitor Login page.

In the case your user name or password are incorrect, a warning appears below the **Sign in** button and you'll have the opportunity to retry.

**Figure 1-1** *Fraud Monitor Login Page*



The screenshot shows the Oracle Communications Fraud Monitor login page. At the top center is the Oracle logo in red. Below it, the text "Communications Fraud Monitor" is displayed in blue. Underneath, there are two text input fields: "Username" and "Password". Below the "Password" field is a "Sign in" button.

## About Using the Fraud Monitor User Interface

The Fraud Monitor user interface has several recurring elements. At the very top, you have the dark bar which gives access to general settings like system information and logout. Below the dark bar on the right is the navigation menu that lets you navigate to the main pages: Overview page, Incidents page, Details page, and the Settings page.

The Overview page shows the current fraud status at a glance. It has big warning indicators as well as a table of the recent potential fraud incidents. From there you can further analyze the latest issues.

The Incidents page displays the full table of recent incidents, with related rules, and from there you can pick an incident for further investigation.

The Details page shows a single user and his incidents. This page contains a short history of the potential fraud that might have occurred.

### Overview Page

The Overview page is the landing page that appears automatically after you log in. The Overview page displays the status information on processed calls, incidents, users, as well as general information about how Fraud Monitor works. You use this page to check for recent incidents and then navigate to other pages to further investigate the user.

[Figure 1–2](#) shows the Overview page.



Figure 1–2 Overview Page

The screenshot displays the Oracle Communications Fraud Monitor interface. At the top, the Oracle logo and 'Communications Fraud Monitor' are visible, along with an 'admin' user dropdown. The main navigation bar includes 'Overview', 'Incidents', 'Details', and 'Settings'. The 'Overview' section is active, showing a 'Status for last hour' with a green checkmark icon, 'Warning: 0', and 'Critical: 0'. Below this, 'Calls Processed Today: 0' is shown. The 'Recent History' section has two tabs: 'Latest Incidents' (selected) and 'Highest Scoring Users'. A table with columns 'Timestamp', '...', 'Score', and 'Level' is present, but it is empty, displaying the message 'There are currently no incidents to show.' The 'How It Works' section contains four numbered steps:

- 1 Rules Defined**: Rules are used to determine what behavior is considered fraudulent and at what severity. Rules read the collected metrics and produce scores.
- 2 Metrics Collected**: Call behavior can be tracked using the metric 'Destination-based Traffic Spikes'.
- 3 Scores Calculated**: The score is the accumulation of values collected for each rule broken. The score is used to compare a user against a 'warning' threshold.
- 4 Incidents Occur**: Surpassing a threshold causes an Incident. Incidents can be 'warning' or 'critical' in nature depending on the severity of the breach. A 'critical' Incident should always be investigated.

### Viewing the Status for the Last Hour

The Status for the Last Hour section displays the total number of calls processed for the day and the number of incidents detected in the last hour. The incident counts are accompanied by large icons for quickly establishing overall status. If no incidents are detected, a large green tick image is displayed. If any warning incidents are detected, a large orange warning sign image is displayed. If any critical incidents are detected, a large red stop sign image is displayed. It's possible for warning incidents and critical incidents to be detected in the same time frame. When an icon is not being displayed, it remains faded grey in the background.

---

**Note:** If the calls processed counter is not increasing, you may not have configured your Mediation Engine correctly.

---

### Viewing the Latest Incidents

On the right-hand side of the page, the Latest Incidents section shows a small list of the most recently detected incidents. A more extensive list can be found on the Incidents page. Double-clicking on an incident will take you to the Details page for that particular offending user.

## Viewing the Highest Scoring Users

On the right-hand side of the page, the Highest Scoring Users section shows a small list of the users with the highest scores. Double-clicking on a user will take you to the Details page for that particular offending user.

## How it Works

On the bottom of the page, the How it Works section outlines how Fraud Monitor works in four steps. You might refer back to this anytime you need to be reminded how the components of Fraud Monitor inter-relate.

## Incidents Page

The Incidents page lists all the calls which have triggered incidents. This includes warning and critical incidents. See the Settings page to configure incident levels. As incidents are triggered they are added to the Incidents page in real-time.

The latest incidents are on top and incidents are not cleared; they stay forever unless you delete them yourself (see below). The **Suspect** column is the callers number or IP address.

---

**Note:** Fraud Monitor captures only the Phone number and not the call conversation.

---

When a line is selected, the panel on the right shows the details of this incident. It displays the caller as well as which rule or rules caused the incident to be triggered.

**Figure 1–3 Incidents Page**

Timestamp	Suspect	Score	Level	Message
Sep 06 11:16	RC_SMC_21.28	1000	CRITICAL	<p>User: 172.16.0.1                      Threshold Exceeded: CRITICAL                      Score: 1000                      Rules Broken: Blacklists                      Date: Sep 06 11:14</p> <p><i>User 172.16.0.1 exceeded the CRITICAL threshold with a score of 1000 points. The user accumulated points by violating the blacklist rule.</i></p> <p>Last call involved in this incident:                      Caller phone number: <a href="#">+493023423604@172.16.0.1</a>                      Callee phone number: <a href="#">+493017500369</a>                      Source IP address: 172.16.0.1                      Destination IP address: 172.16.0.2                      SIP User-Agent: Unknown</p>
Sep 06 11:16	10.13.21.28	1000	CRITICAL	
Sep 06 11:16	<a href="#">+18005781245@10.13.21.28</a>	1000	CRITICAL	
Sep 06 11:14	swisscom.ch	1000	CRITICAL	
Sep 06 11:14	172.16.0.1	1000	CRITICAL	
Sep 06 11:14	<a href="#">+493023423604@172.16.0.1</a>	1000	CRITICAL	
Sep 06 11:14	<a href="#">+493020666574@172.16.0.1</a>	1000	CRITICAL	
Sep 06 11:14	<a href="#">+493005656309@172.16.0.1</a>	1000	CRITICAL	
Sep 06 11:14	<a href="#">+41219030350@swisscom.ch</a>	1000	CRITICAL	

If you double-click on an incident, you'll go to the Details page for that user. Selecting a row and clicking **Go to User Details** button does the same.

If a user first triggers a *warning* incident and later upgrades that to a *critical* incident, both will be listed.

You can delete an incident by selecting it and clicking **Delete**. This will remove the incident from the list. When user causes multiple incidents of the same level (warning or critical) within 24 hours, a new incident is not triggered. Deleting a row from the incident list will *not* reset that timer. Deleting an incident is useful when, after investigation, you conclude that an incident is not fraudulent.

Times are in the local time zone.

## Details Page

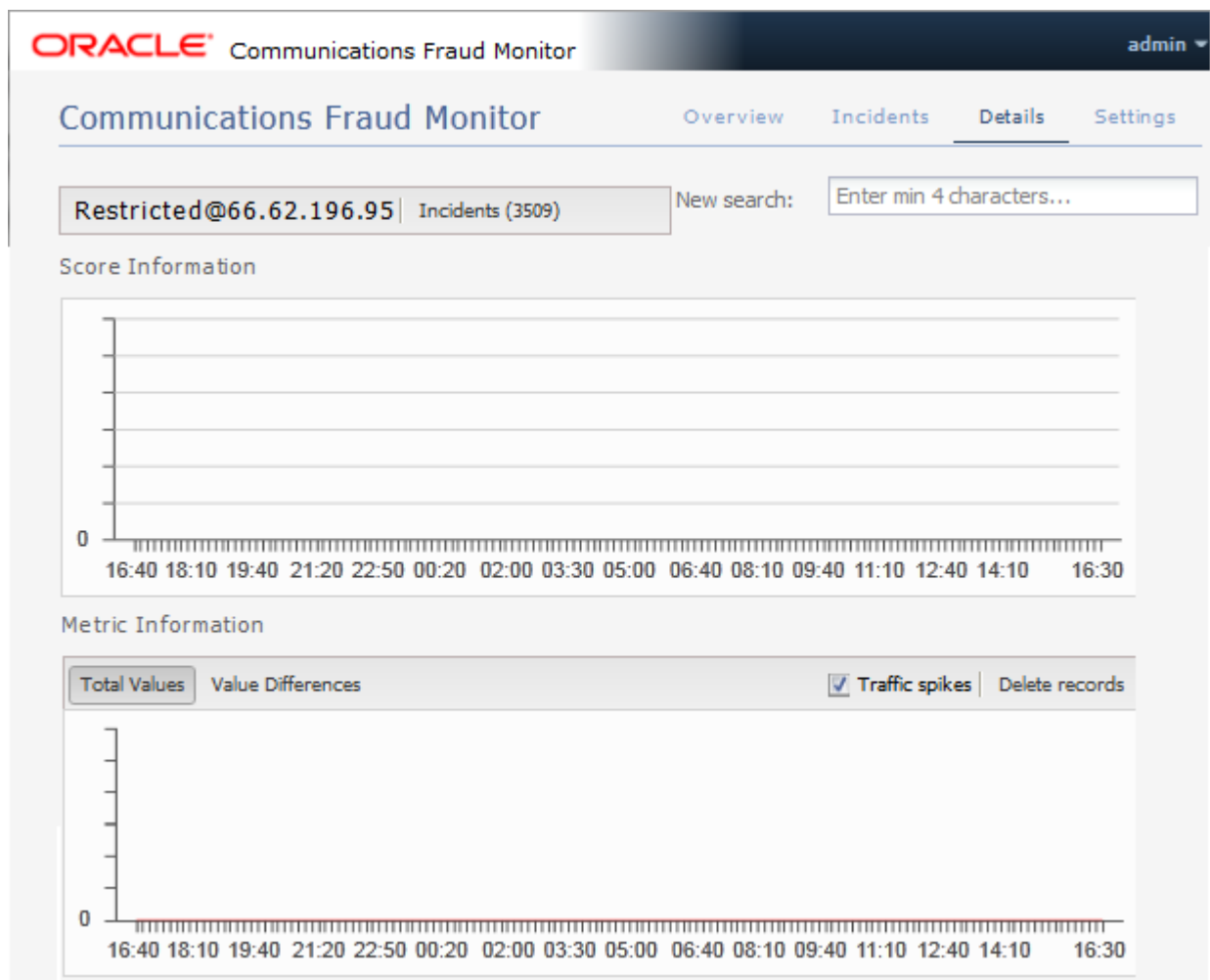
The Details page shows information on a particular user. Also, the whitelist for countries of this user can be maintained on this page and all records associated with this user may be deleted.

Figure 1–4 shows the Details page.

The Details page can be reached via the top menu or from the Incidents page.

Typically, in this view one will search a user, if none is selected yet, and then consider the metrics to determine if an incident is justified. In case no user has been chosen, one must be selected using the search field. Then the scores, the calls, and the geographical data for this user are displayed. Each of these topics is explained in the following sections.

**Figure 1–4** Details Page



### Performing a User Search

The **New search** field allows you to select a user for display by IP or phone number. After four characters matches are shown. Select one of the proposed matches, press return or click **Search** to display the user.

### Deleting User-Specific Records

Click **Delete records** to remove all information regarding the user. This includes metric values, scores and incident related information.

### Viewing Score Information

The Score Information diagram shows scoring information of all incidents for the last 24 hours, going back from the current time. It is not possible to go further back than 24 hours. For each incident measuring interval, a bar displays the score reached.

### Viewing Metric Information

The Metric Information diagram show metrics of selected rules. For each ten minute interval, the values of the last 24 hours are shown in comparison to the average over the last two weeks.

The y-axis displays the number of minutes or calls, while the x-axis specifies the intervals. A red line displays the averages, while the bars show the current data.

By using the check boxes in the top right corner, you can choose what values to display.

- The traffic spikes

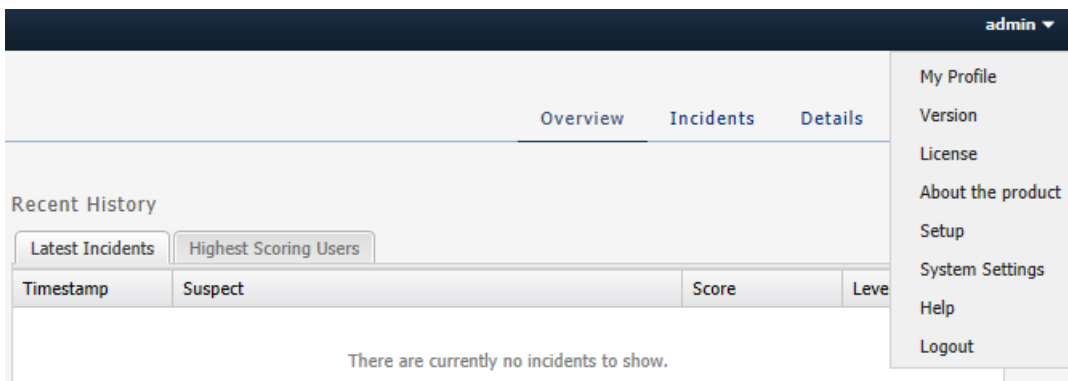
The alternative display modes in the top left corner, **Total Values** and **Value Differences**, toggle between displaying the current values as absolute values and as the difference to the average.

## User Menu

The User menu is located on the top right corner of the page on the header bar. A drop-down menu appears when you click on your user name.

Figure 1-5 shows the User menu.

Figure 1-5 User Menu



## Editing the User Profile

You can edit your own profile details by selecting **My Profile** in the User menu. A dialog box appears giving you the option to change your user name, email and password. Fill out the new values for the details you would like to change and click **Finish** to save the changes. Click **Cancel** to exit the window without making changes.

## Viewing System Information

You can view the current system information by selecting **System Info** in the User menu.

## Viewing License Information

You can view the product license terms and conditions by selecting **License** in the User menu.

## Logging Out

You can logout of Fraud Monitor by selecting **Logout** in the User menu. This brings you back to the Login page.

## Settings Page

The Settings page of the Fraud Monitor user interface lets you configure the rules, manage the users, adapt the notifications, specify blacklists, whitelists, ratelimit, redirect, import/export lists, and generate automatic lists required for a successful operation of Fraud Monitor.

Among the settings, rules is the most important setting. In the Rules section, you can enable and configure patterns that are used to detect fraud and trigger incidents.

The screenshot displays the Oracle Communications Fraud Monitor interface. The top navigation bar includes 'Overview', 'Incidents', 'Details', and 'Settings'. The main content area is titled 'Communications Fraud Monitor' and features a 'Destination-based traffic' checkbox which is checked. Below this, there is a table for rule configurations:

Point Type	Threshold	Points	Familiarity Limit
Dynamic	50%		>120
Static	5000	300	

Below the table are sections for 'Rule Filters' and 'Rule Weight'. The 'Rule Weight' section shows a 'Weight' dropdown menu set to '1.00' and a 'Save' button. On the right side, there is a sidebar with a 'Rules' section containing a list of rule types: 'Destination-based traffic spikes', 'Call Volume', 'Notifications', 'Blacklist', 'Whitelist', 'Ratelimit', 'Redirect', 'Setup', 'Import/Export', and 'Automatic List'.



---

---

## About Detecting Fraud

This chapter describes some of the common fraud scenarios and fraud detection rules.

### How Fraud Monitor Detects Fraud

The Session Monitor probes and Oracle Communications Session Border Controllers with the embedded probes software enabled send monitoring information to the Mediation Engines. The Mediation Engine (ME) then feeds call state information to Fraud Monitor. Fraud Monitor analyzes every incoming call and applies various rules to them. A single rule or a combination of multiple rules may add enough points to trigger a fraud alert. Alerts are on two levels: *warning* and *critical*. Warning level alerts should be investigated while critical level alerts can be considered proven fraud incidents, for example, due to hits on the blacklist which contains known incidents.

---

---

**Note:** A user (also known as a subscriber to distinguish between users of the system and participants in monitored calls) is identified either by his IP address or by the local part of his From SIP URI. If the SIP URI is sip:2125551234@example.com, then the user is shown as 2125551234 in the GUI.

---

---

### About Fraud Scenarios

The following sections describe some of the common fraud scenarios.

#### PBX Fraud

##### Scenario

Users on the internal side (for example, inside an enterprise) may conduct outbound calls and also receive calls. When looking from the outside (visible to Session Monitor or an SBC), the PBX receives calls for a limited set of numbers (for example, the number range of the enterprise) and makes phone calls to almost any number. Depending on the customer, the outbound calls may be directed to a restricted area (for example, mostly local calls).

##### Detection Method

Whenever possible, multiple metrics should be used to identify fraud. Calls bound to the PBX (as seen from Session Monitor or an SBC) are not subject to fraud in this context but may be part of a fraud scheme (for example, when representing the inbound leg of a forwarded call). In fact, an attacker might bypass the Session Monitor or the SBC monitoring points so that inbound calls are not. Fraud might be detected by

observing a change in the daily distribution of calls as well as the geographical restrictions.

## International Revenue Share Fraud

International Revenue Share Fraud (IRSF), Domestic Revenue-Share Fraud (DRSF), and Premium Rate Fraud are closely linked. The detection methods for all three scenarios are similar and all covered in this section.

### Scenario

An attacker operates a premium number with a revenue share provider in a foreign country. For each call or call minute conducted to this number the attacker receives part of the revenue. The attacker's goal is to inflate the traffic to this number to increase his revenue. The services provided via this number may range from random announcements to call-through services. To redirect traffic to his number, the attacker may place calls (no connect, just creating a missed call entry) with a spoofed number to victims leading them to call him back. In a more sophisticated scenario, the attacker introduces his premium number into his victims' communication as a call-through service. He may modify VoIP endpoints (PBXes, VoIP enabled routers, and so on.) to carry his number as prefix. A Bluetooth-based attack has been used to replace phone numbers in mobile phones and prefix them with a premium number. This not only increases the revenue for the attacker, but (as above) also allows the attacker to eavesdrop on the phone calls. The most common approach to inflate traffic to the fraudsters phone number is to break into PBX or voicemail systems and call his own number knowing that this costs the PBX or voicemail operator significant amounts of money.

Typically the fraudster can collect revenue from the premium number quicker (for example, each day or each week) than the billing cycle on the originating side (for example, once a month). This allows the fraudster to extract money from the system before the bill hits him on the originating side if he decides to increase the traffic on his own.

### Detection Method

The Amount of Traffic to the fraudulent number(s) increases. A hit on the Blacklist may also be triggered.

## About Fraud Detection Rules

The metrics described in this section are based on the fraud scenarios above. Multiple rules may be combined to detect a single fraud scenario. Throughout this section the term subscriber relates to either a single IP address or a single phone number.

### Traffic Profile

Once a few days of call data for a single subscriber is available a graph with the time of the day on the x-axis may be generated. The y-axis shows the number of calls or call minutes conducted. Once a fraud attack happens the shape of the graph will change.

### Blacklist and Whitelist Entries

A list of specifically allowed and disallowed phone numbers or phone number prefixes can be used to identify fraudulent calls. In case international entries are disallowed by a company policy, an international entry may be an indicator of fraud. The customer may add individual entries to a customer-specific blacklist.



Depending on whether the system observed an exact entry hit or a prefix match the scores assigned may differ. A prefix match on its own may not directly trigger a critical alarm but when combined with other metrics (for example, the amount of traffic to the suspicious entry) it may generate a critical alarm.

### **Destination-Based Traffic Spikes**

Fraud Monitor can raise an incident if a given destination user receives unusually high traffic, as in an IRSF scenario. If a configurable threshold is exceeded, both the source and destination users accumulate points. This rule can be used to identify possible candidates for blacklisting destination numbers.



---

---

## Installing Fraud Monitor

This chapter describes how to install Oracle Communications Fraud Monitor.

### Hardware Requirements

The following minimum requirements must be met to install Fraud Monitor:

- 2.6 GHz Intel Xeon processor, 64-bit with 8 processing threads
- 8 GB RAM
- 70 GB storage on a hardware RAID controller
- 2 Ethernet ports

---

---

**Note:** For production use, Oracle recommends a more thorough sizing exercise completed with your Oracle sales engineer. Higher performance hardware may be required, for example, in cases with:

- High levels of monitored traffic
  - High numbers of concurrent users
  - High volumes of historical information
- 
- 

### Installing Fraud Monitor

To install Fraud Monitor:

1. Install Session Monitor using RPM. Refer to Installing Session Monitor using RPM in the *Session Monitor Installation Guide*.
2. Login to Platform Setup Application (PSA) and configure the machine as Fraud Monitor. Refer to the section, About the Platform Setup Application in *Session Monitor Installation Guide*.
  - a. On the Machine Type screen, select **Aggregation Engine**.
  - b. Select **Fraud Monitor**.

Follow the steps in the Installation wizard.

After successful installation, the user should be able to login to the application with Default credentials. Contact your Oracle Sales Representative.



---

---

## Configuring Fraud Monitor

This chapter provides information for configuring Oracle Communications Fraud Monitor.

### About Configuring Fraud Detection Rules

The Settings page of the Fraud Monitor user interface lets you configure the rules, manage the users, adapt the notifications, specify blacklists, whitelists, ratelimit, redirect, import/export lists, and generate automatic lists required for a successful operation of Fraud Monitor.

The Rules section enables you to configure the patterns that are used to detect fraud and trigger incidents. If the current settings do not trigger any incidents, you may need to change the patterns or raise the points.

---

---

**Note:** Go to the Platform Setup Application and refer to *Session Monitor Installation Guide* for settings (for example, network interfaces, DNS, or SMTP) that affect the server running Fraud Monitor.

---

---

### Configuring Rules

Fraud Monitor raises an incident if a given destination user receives unusually high traffic, as in an IRSF scenario. For each call, Fraud Monitor monitors the total number of minutes that the destination user has received the traffic and compares it to its historical average. If a configurable threshold is exceeded, both the source and destination users accumulate points. This rule can be used to identify possible candidates for blacklisting destination numbers.

#### Call Volume:

Fraud Monitor can raise an incident if a given destination user receives unusually high traffic rate as measured by **Success Calls Per second** or **Max Active Calls**.

For each call, Fraud Monitor, monitors the **Success Calls Per Second** that the destination user has received and compares it to its historical average (Success Calls are when 200OK for INVITE is received).

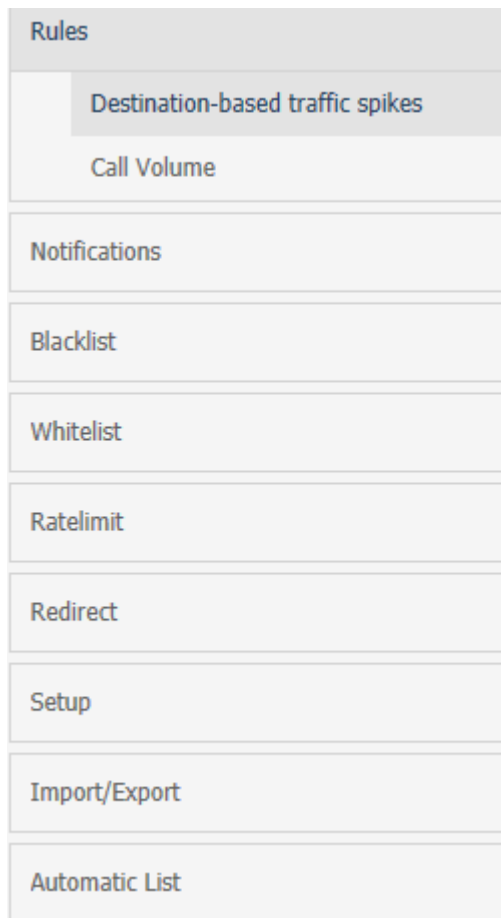
Simultaneously, it also monitors the Active Calls for that user. If a configurable threshold is exceeded for either Calls per second OR Max Active Calls, both the source and destination users accumulate points. This rule can be used to identify possible candidates for blacklisting or redirecting destination numbers.

Fraud Monitor uses configurable rules to find call patterns which are considered fraudulent and classify the severity of the incident with a points system. On the Rules section, you can decide which rules are used, configure them, and restrict their use.

The navigation bar on the right-hand side of the page lists the pre configured fixed set of rules you can use.

Figure 4–1 shows the navigation bar on the Settings page.

**Figure 4–1 Navigation Bar on the Settings Page**



Clicking on a rule opens up its configuration panel in the left column. Use the check boxes next to the rule name in the left column to enable and disable the rule.

Figure 4–2 shows an example of rules configuration.

Every configuration panel has **Add**, **Edit** and **Delete** buttons, which you can use to configure that specific rule. A brief help text is shown above the panel to aid you in the configuration process.

Every rule is assigned a weight. The default is **1.00**. The rule weight can be used to make some rules more important than others.

To restrict the applicability of the rule, select the **Rule Filters** checkbox and enter the caller or callee information in the dialog box.

Figure 4–2 Example of Rules Configuration

**ORACLE** Communications Fraud Monitor admin

Communications Fraud Monitor Overview Incidents Details Settings

Destination-based traffic spikes ?

This rule catches traffic spikes based on absolute amounts (static rule) or deviations from the typical traffic pattern (dynamic rule). Use the filtering mechanism to limit this rule to specific destinations (e.g. countries) or for instance all international calls.

Point Type	Threshold	Points	Familiarity Limit
Dynamic	50%		>120
Static	5000	300	

**Rule Filters** ?

Type	Match Value	Redirect Target

**Rule Weight**

The weight applied to the rule defines how severely positive matches are scored.

Weight:  Save

**Rules**

Rules are used to determine what call behavior is considered fraudulent and at what severity. A rule can make use of any number of metrics and determines how values are attributed to each user.

To disable a rule, uncheck the checkbox preceding the rule's name. When a rule is disabled, the corresponding data will cease to be collected.

**Rules**

- Destination-based traffic spikes
- Call Volume
- Notifications
- Blacklist
- Whitelist
- Ratelimit
- Redirect
- Setup
- Import/Export
- Automatic List

## Setting Up Email Notifications

When Fraud Monitor detects an incident, it notifies the users by email.

Figure 4–3 shows an example of the notification settings.

To send e-mail notifications, click on **Add recipient...** In the window that appears, enter the following settings:

- **Name:** A name to identify the new entry in the list of recipients
- **Email:** The email address to which notifications will be sent
- **Incident level:** Select **WARNING + CRITICAL** to receive all notifications, or **CRITICAL** to only receive notification on critical incidents
- **Prefix:** Emails from the system will contain this prefix in the **Subject:** field of the recipient inbox

Figure 4–3 Notification Settings for an Email Recipient

**Email Recipients**

Name	Email	Incident level	Prefix
admin	test@example.com	WARNING	

**SNMP Notifications**

Type	SNMP Engine id	SNMP User Name	Host	Port	Community	Incident level
No SNMP recipients have yet been configured.						

**Notification Thresholds**

WARNING:  Save

CRITICAL:  Save

The thresholds are in relation to the maximum score a user needs to accumulate before OCFM sends out a notification. Ensure your thresholds are in accordance with any custom defined rules.

During OCFM's learning period points may be attributed too freely and you may receive more notifications than necessary. Over time OCFM will distribute fewer points more accurately, therefore the threshold will be relatively low.

Set the notifications thresholds based on what level of learning OCFM is at. (e.g., the thresholds may start at 1000, and settle down to 100)

Download here the [MIB definition for OCFM SNMP notifications](#). This file can be used within your network management tools.

**Rules**

- Notifications
- Blacklist
- Whitelist
- Ratelimit
- Redirect
- Setup
- Import/Export
- Automatic List

## Adjusting the Notification Levels

To receive more or less notifications, you can adjust the two levels, warning and critical, in number of Incident points. The rules specified in the Rules page assign points to each user of the network. If the number of points for a user exceeds the

threshold warning (1000 by default), an email is sent to all recipients of level **WARNING**. If it exceeds the level critical (1500 by default), the notification is sent to all recipients.

This is a global sensitivity adjustment. You can choose the amount of points each single rule attributes in the Rules section.

## Specifying Blacklist

The Blacklist contains phone numbers, IP addresses, and hostnames which have been verified in fraudulent activity. You can enable and disable the Blacklist feature for specific data types in the configuration menu.

The Blacklist information provided by Oracle is in the international format. You can append a prefix to international numbers or provide a regular expression to transform the number.

The Global Blacklist is read-only and can be uploaded using the **Update** menu. You can also add and remove individual entries in the Custom Blacklist area.

## Specifying Whitelist

You can add and remove whitelist entries. Both IP addresses and phone numbers are possible. After adding or removing white-list entries, click **Save**. The new rules will go into effect immediately.

Phone numbers or IP addresses matching a whitelist entry are not used for point calculation. This filtering is done before any processing by any rule.

Calls which match a whitelist entry can still raise incidents. For example, if you block a certain caller IP address a call can still trigger an incident if the callee phone number is on the blacklist.

Both the phone number and the IP address of the caller and of the callee are tested against the list. The comparison is against the complete value, so there are no regular expressions or substring comparisons. If there are alphanumeric letters in the number, these will be treated as case sensitive.

Some rules only check against the caller's IP address or phone number. Filtering based on values you would expect in the callee won't significantly effect these rules.

## Specifying Ratelimit List

The Ratelimit allows you to add the custom entries. You can add Phone numbers, IP addresses, User names and SIP User Agents. You can also exempt users by removing them from the global ratelimit.

Customers may either upload the ratelimit information provided through the import menu or they can manually enter the custom entries.

Global flag is marked as **True** for entries uploaded through import menu such as the phone numbers, usernames, hostnames, and SIP User Agents which have been identified and verified to be involved in fraudulent activity.

Use the Configuration menu to adjust the points awarded for prefix and exact match hits from this list.

Should you want to exempt a specific entry, check the corresponding flag while adding or modifying that entry. But that exemption does not work for other lists like blacklist or redirect. If you want to exempt an entry from all lists, add the same in



Whitelist. The CPS or MAC entries are not taken into account for raising incidents from ratelimit list, only presence is checked.

Entry can also come in this list via Automatic Configuration: Subscribed flag would be true for such entries and also those entries cannot be used for raising further incidents.

The Ratelimit supports all the data types supported by SBC for processing the calls. Following are the available data types:

- from-hostname
- to-hostname
- from-phone-number
- to-phone-number
- from-username
- to-username
- user-agent-header

The Ratelimit List allows addition of custom entries to configure a limit on Calls per second and maximum active calls from suspicious users. You can add phone numbers, hostnames, usernames and user-agent headers. Here you can also exempt users.

Type	Match Value	Calls Per Second	Max Active Calls	Date	Subscribed	Global	Comment
From-hostname	172.16.0.2	4	5	2018-10-03 09:36:39	Yes	No	
From-phone-number	+493018488376	4	5	2018-10-03 09:38:43	Yes	No	
From-phone-number	+49306454864	4	5	2018-10-03 09:38:43	Yes	No	
From-hostname	172.16.0.3	4	5	2018-10-03 09:38:43	Yes	No	
From-phone-number	+49306074032	4	5	2018-10-03 09:38:43	Yes	No	
From-phone-number	+493022141519	4	5	2018-10-03 09:38:43	Yes	No	
From-phone-number	+493011453894	4	5	2018-10-03 09:38:43	Yes	No	
From-phone-number	+49305735294	4	5	2018-10-03 09:38:44	Yes	No	
Total entries: 9121		Displaying the first 25 entries, search above for more.					

You can filter the data based on these data types. Click the required data type in the screen and data is displayed for the selected data type.

You can **Add**, **Edit**, and **Delete** the users. Double-click a user to edit the details.

## Adding a Ratelimit User

You can add a ratelimit user and specify the data type. Fraud Monitor captures the information for the user based on the data type.

To add a ratelimit user:

1. From the **Settings** screen, click **Ratelimit**.  
The Ratelimit screen appears.
2. click **Add**.  
Add a Ratelimit User screen appears.
3. From the **Type** drop-down list select the data type for the user.
4. In the **Match Value** field, enter the value of the type selected above. The value depends on the **Type**.  
For example, if you have selected, **from-phone-number** for the **Type**, then the **Match Value** must be a valid phone number.
5. In the **Calls Per Second** field, enter the number of seconds that call shall be allowed.

6. In the **Max Active Calls** field, enter the number of calls allowed for the user from the **Type** selected.
7. In the **Comment** field, enter any additional information for the user.
8. (Optional) Select **User exempted from ratelimit** to exempt from ratelimit.

---

**Note:** By selecting this option, you are exempting the user from the global ratelimit. Fraud Monitor remains susceptible to accumulating points from other rules defined for the user.

---

9. Click **Save** to add the user or click **Cancel**.

## Configuring Ratelimit

Configuring Ratelimit screen allow you to enable and disable the Ratelimit feature for specific data types, such as Phone numbers, IP addresses, User Names or SIP User Agents. Disabling a data type has an effect on Ratelimit List. You may assign points for both prefix and exact hits for each data type.

	Prefix match	Exact match	Enabled
Phone numbers	750	1000	<input checked="" type="checkbox"/>
from-phone-number			
to-phone-number			
IP addresses		1000	<input checked="" type="checkbox"/>
from-hostname			
to-hostname			
User Names		1000	<input checked="" type="checkbox"/>
from-username			
to-username			
user-agent-header		1000	<input checked="" type="checkbox"/>

---

**Note:** You have to modify **Current Notification Thresholds** from **Notifications** screen.

---

## Specifying Redirect List

The Redirect allows you to add the addition of custom entries. You can add Phone numbers, IP addresses, User names and SIP User Agents. You can also exempt users by removing them from the global redirect list.

Customers may either upload the redirect information provided through the import menu or they can manually enter the custom entries.

Global flag is marked as **True** for entries uploaded through import menu such as the phone numbers/usernames, hostnames, and SIP User Agents which have been identified and verified to be involved in fraudulent activity.

Use the Configuration menu to adjust the points awarded for prefix and exact match hits from this list.

Should you want to exempt a specific entry, check the corresponding flag while adding/modifying that entry. But that exemption will not work for other lists like Blacklist or Ratelimit. To exempt an entry from all lists, add the same in Whitelist.

Entry can also come in this list via Automatic Configuration: Subscribed flag would be true for such entries and also those entries are not meant to be used for raising further incidents.

The Redirect supports all the data types supported by SBC for processing the calls. The available data type are:

- from-hostname
- to-hostname
- from-phone-number
- to-phone-number
- from-username
- to-username
- user-agent-header

You can filter the data based on these data types. Click the required data type in the screen and data is displayed for the selected data type.

You can **Add**, **Edit**, and **Delete** the users. Double-click a user to edit the details.

**Figure 4–4 Redirect List**

The screenshot shows the 'Redirect List' section of the Communications Fraud Monitor. It includes a search bar and a table with the following data:

Type	Match Value	Redirect Target	Date	Subscribed	Global	Comment
from-phone-number	+132127458	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127459	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127460	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127461	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127462	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127463	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127464	10.11.121.10	2018-10-03 08:36:29	No	Yes	
from-phone-number	+132127465	10.11.121.10	2018-10-03 08:36:29	No	Yes	
Total entries: 100						

## Adding a Redirect User

You can add a redirect user and specify the data type. Fraud Monitor captures the information for the user based on the data type.

To add a redirect user:

1. From the **Settings** screen, click **Redirect**.

The Redirect screen appears.

2. click **Add**.

Add Redirect User screen appears.

3. From the **Type** drop-down list select the data type for the user.
4. In the **Match Value** field, enter the value of the type selected above. The value depends on the **Type**.

For example, if you have selected, **from-phone-number** for the **Type**, then the **Match Value** must be a valid phone number.

5. In the **Redirect Target** field, enter the IP address to redirect the call.
6. In the **Comment** field, enter any additional information for the user.

- (Optional) Select **User exempted from redirect** to exempt from redirect.

---

**Note:** By selecting this option, you are exempting the user from the global redirect. Fraud Monitor remains susceptible to accumulating points from other rules defined for the user.

---

- Click **Save** to add the user or click **Cancel**.

## Configuring Redirect

Configuring Redirect screen allow you to enable and disable the Redirect feature for specific data types, such as Phone numbers, IP addresses, User Names or SIP User Agents. Disabling a data type has an effect on Redirect list. You may assign points for both prefix and exact hits for each data type.

Redirect Configuration

This page allows to enable and disable the Redirect feature for specific data types, i.e. phone numbers, hostnames, usernames or user-agent headers.

**Current Notification Thresholds**  
 WARNING: 750  
 CRITICAL: 1000  
Note! Changes to the notification thresholds can be made on the Notifications page.

Data Type	Prefix match	Exact match	Enabled
Phone numbers	750	1000	<input checked="" type="checkbox"/>
IP addresses	750	1000	<input checked="" type="checkbox"/>
User Names		1000	<input checked="" type="checkbox"/>
user-agent-header		1000	<input checked="" type="checkbox"/>

Save

---

**Note:** You have to modify **Current Notification Thresholds** from **Notifications** screen.

---

## Configuring Mediation Engine

The configuration section under Setup lists the Mediation Engine connections. Fraud Monitor analyzes the data from the connected Mediation Engines.

The Fraud Monitor details needs to be configured at Mediation Engine. See the section *Configuring Fraud Monitor*, in *Operations Monitor User's Guide*.

Once the connection is established between Mediation Engine and Fraud Monitor, the connection details are displayed in this configuration screen. You can also view the connection failures details on this page.

- **Name:** Indicates the machine name.
- **IP:** Indicates the IP address to which Fraud Monitor tries to connect for analyzing the data.
- **Status:** Indicates whether the Mediation is connected or disconnected.
- **Date:** Indicates the date and time when the Mediation Engine is connected or disconnected.

After adding or changing a connection, Fraud Monitor tests the connection. Any errors will display in a dialog box.

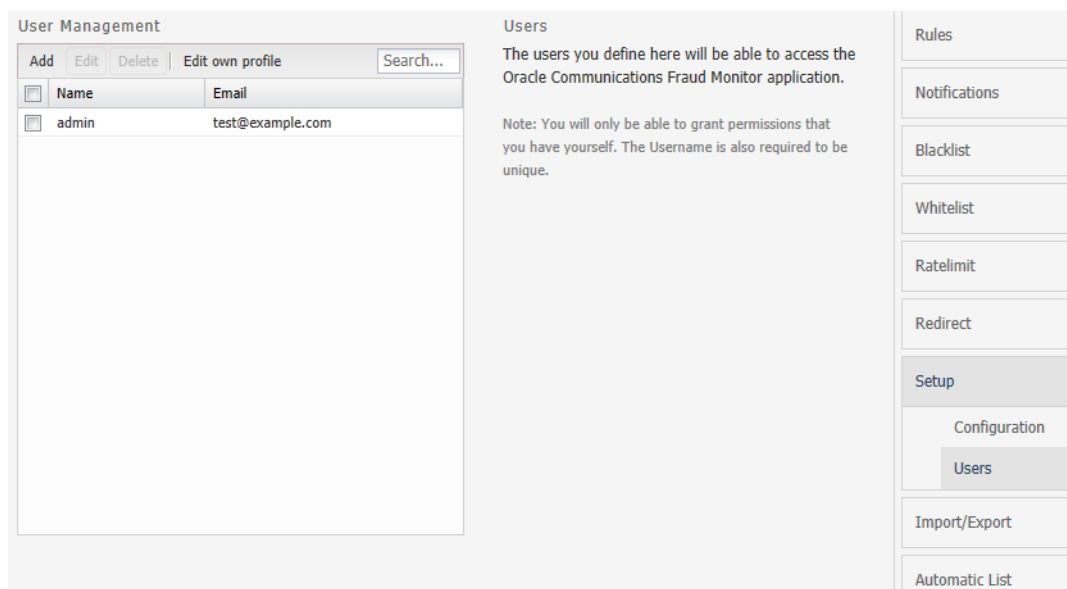
## Managing Users

You can manage users and assign permission for accessing the Fraud Monitor information. You can create user accounts to work with Fraud Monitor.

By default, only the *admin* account exists. The admin can **Add**, **Edit**, and **Delete** the users.

Figure 4–5 shows an example of the users list.

**Figure 4–5** Users List



To add an user:

1. From **Settings** page, click **Setup**.
2. Click **Add**.  
The Add User screen appears.
3. In this screen, do the following:
  - a. In the **Username** field, enter the user name for the new account.
  - b. In the **Email** field, enter the e-mail address of the user.
  - c. In the **New Password** field, enter the password for the user account.
  - d. In the **Repeat Password** field, re-enter the password from the above step.

Click **Next**.

The Add User - Permission Settings screen appears.

4. Select the permissions for the user by clicking the checkbox. Alternatively, you can click **check all** and **uncheck all** options.

User is created successfully. You can edit user details by clicking the **Edit** button.

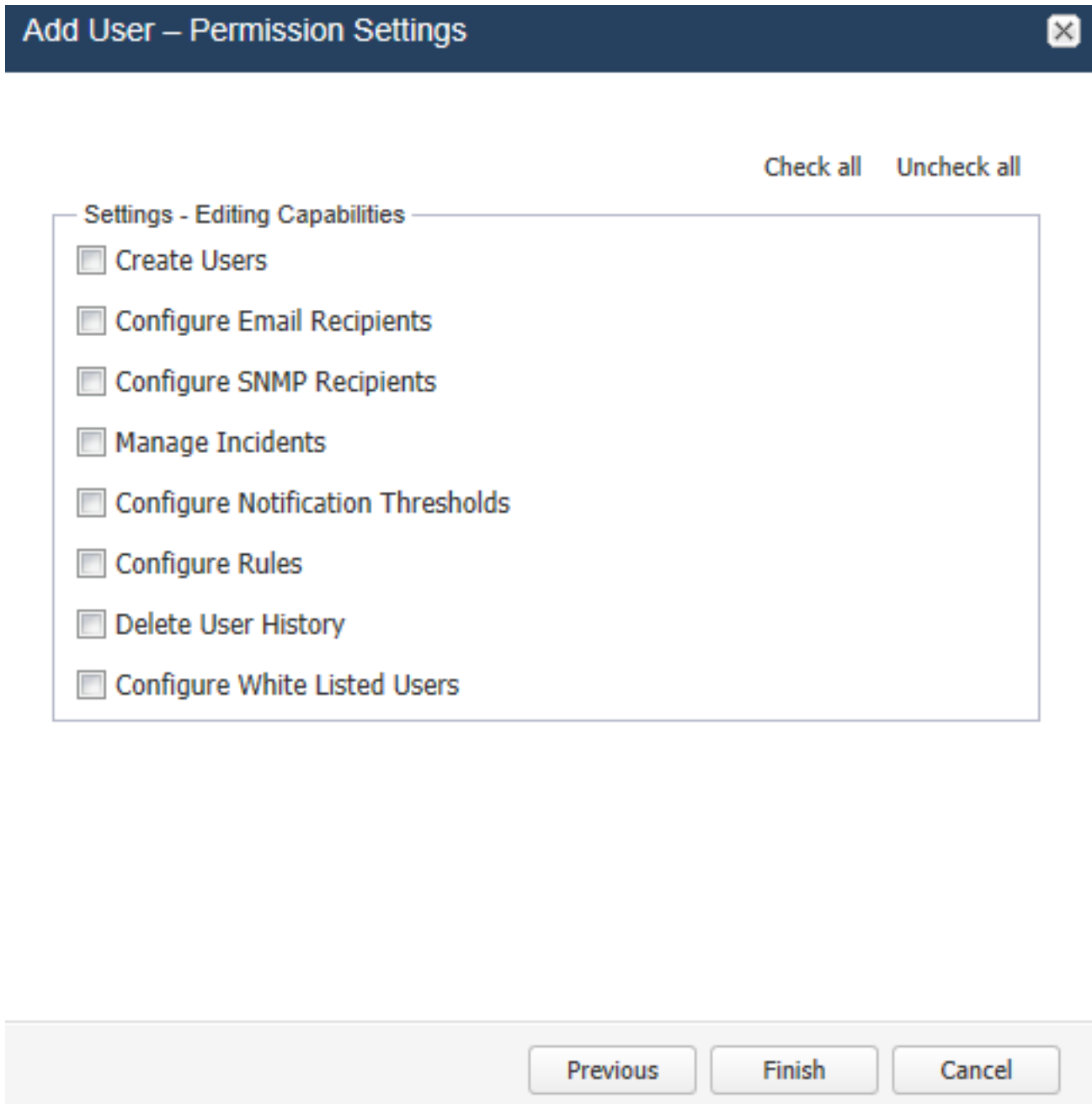
---

**Note:** The new user will then be able to connect using the credentials you have chosen. It is recommended that the user change this password at the first connection.

---

Figure 4–6 shows the user permission settings.

Figure 4–6 Granting Capabilities to the New User



## Configuring Import/Export

The Import/Export allows you to import/export data in CSV format for a particular list type (Blacklist/Ratelimit/Redirect).

---

---

**Note:** You can only import/export files in .csv format. Maximum file size allowed is 10 MBytes.

---

---

Import/Export

This page is used to import/export data in CSV format to particular list type(Blacklist/ Ratelimit/ Redirect) selected.  
 Note: Accepts only csv format & Maximum allowed file size is 10Mb.

**Number Prefix:**  
 The Blacklist, Ratelimit & Redirect information is in the international format without a leading + or leading zeros. If you use a different numbering scheme in your network please provide the prefix to prepend to numbers or a regular expression to transform the numbers.

Enter prefixes below:

Keep original numbers (without prefix) in list

---

**Import**

List Type:

---

**Export**

List Type:

From this screen, you can:

- Number Prefix:** You can enter prefixes of the phone numbers to save the data for exporting and importing. The Blacklist information is in the international format without a leading + or leading zeros.  
 If you use a different numbering scheme in your network, provide the prefix to prepend to the international numbers or a regular expression to transform the numbers.
- Import:** Import either Blacklist, Ratelimit, or Redirect lists. You can select the required option from the drop-down list and **Select file** from your system and click **Upload** for importing the file.
- Export:** Export either Blacklist, Ratelimit, or Redirect lists. You can select the required option from the drop-down list and click **Export** for exporting the file.

## Configuring Automatic List

In Fraud Monitor, you can configure different threshold for different lists (Blacklist, Ratelimit, and Redirect) based on the metric rules, Destination Based Traffic Spikes/Call Volume.

When the configured threshold is reached, the corresponding suspicious user/Phone number is moved automatically to the respective list as configured.

Automatic List

Rules	Actions	Threshold	Value
Destination-based traffic spikes	<input type="checkbox"/> Blacklist	0	
	<input type="checkbox"/> Redirect	0	Redirect Target: <input type="text"/>
	<input type="checkbox"/> Ratelimit	0	Calls Per Second: <input type="text"/> Max Active Calls: <input type="text"/>
Call Volume	<input type="checkbox"/> Blacklist	0	
	<input type="checkbox"/> Redirect	0	Redirect Target: <input type="text"/>
	<input type="checkbox"/> Ratelimit	0	Calls Per Second: <input type="text"/> Max Active Calls: <input type="text"/>

Automatic List

Fraud Monitor can configure different threshold for different lists (Blacklist, Ratelimit and Redirect) based on the metric rules (Destination Based Traffic Spikes / Call Volume). When the configured threshold is reached the corresponding suspicious user/Phone number would be moved automatically to respective list as configured.

Rules

Notifications

Blacklist

Whitelist

Ratelimit

Redirect

Setup

Import/Export

Automatic List





---

---

# Glossary

## **IRSF**

International Revenue Share Fraud is a fraud scenario in which the fraudulent user earns money by directing lots of traffic to his or her own revenue share numbers.

## **Probe**

A machine which filters and processes network traffic. It doesn't calculate the statistics.

## **PBX**

Private Branch Exchange is a telephone exchange (often SIP based) that connects a business to a VoIP carrier (Communication Service Provider).

## **RTP**

Real-time Transport Protocol. Used for transporting media. Defined in **RFC 3550**. For more information, see the IETF Tools website at:

<http://tools.ietf.org/html/rfc3550.html>

## **VLAN**

Virtual Local Area Network is a technique to separate a network into distinct, isolated broadcast domains.

See [https://en.wikipedia.org/wiki/Virtual\\_LAN](https://en.wikipedia.org/wiki/Virtual_LAN).

