# Oracle® Communications Session Monitor

## Fraud Monitor User Guide

Release 4.3
F27696-01
March 2020

ORACLE

Oracle Communications Session Monitor Fraud Monitor User Guide, Release 4.3

F27696-01

# Contents

## 2 Detecting Fraud



## 3 Installing Fraud Monitor



## 4 Configuring Fraud Monitor

# About This Guide

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

**Documentation Set**

| Document Name | Document Description |
|---|---|
| Developer Guide | Contains information for using the Session Monitor SAU Extension. |
| Fraud Monitor User Guide | Contains information for installing and configuring Fraud Monitor to monitor calls and detect fraud. |
| Installation Guide | Contains information for installing Session Monitor. |
| Mediation Engine Connector User Guide | Contains information for configuring and using the Mediation Engine Connector. |
| Operations Monitor User Guide | Contains information for monitoring and troubleshooting IMS, VoLTE, and NGN networks using the Operations Monitor. |
| Release Notes | Contains information about the Session Monitor 4.3 release, including new features. |
| Security Guide | Contains information for securely configuring Session Monitor. |
| Upgrade Guide | Contains information for upgrading Session Monitor. |

# Revision History

This section provides a revision history for this document.

| Date | Description |
|---|---|
| March 2020 | OCSM 4.3 Release |

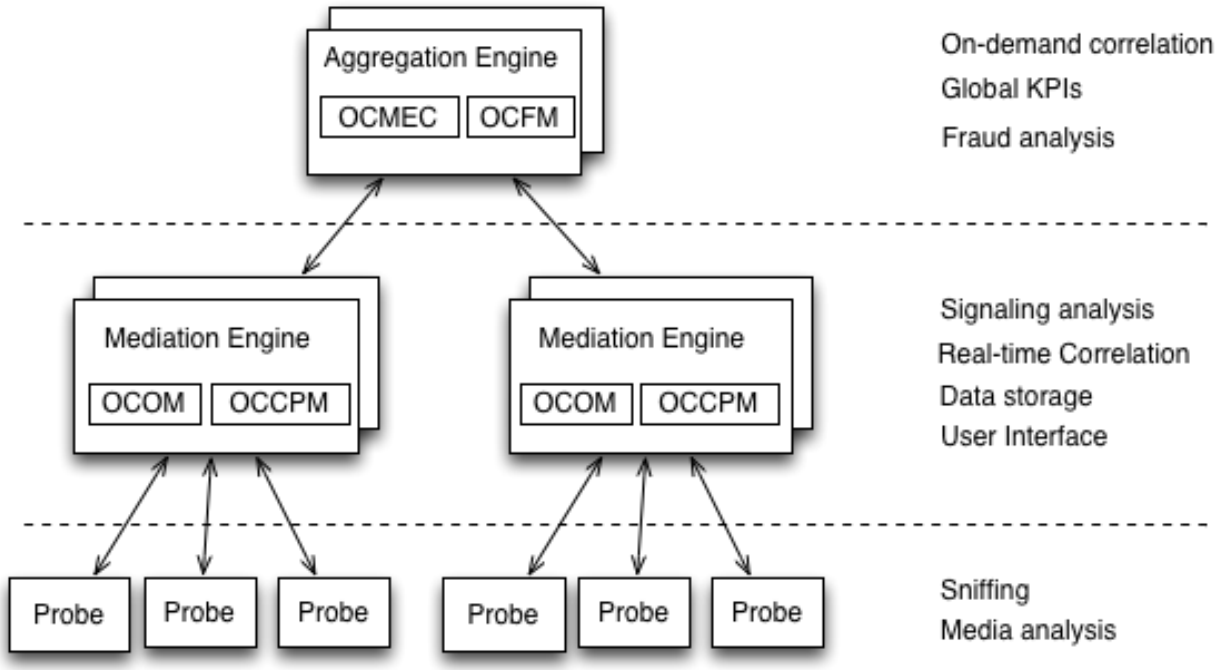
# 1
# Overview of Fraud Monitor

This chapter provides an overview of Oracle Communications Fraud Monitor.

## About Fraud Monitor

Oracle Communications Session Monitor captures network traffic, correlates it in real time, and stores it in an indexed format for reporting by the browser interface. A multi-layered architecture ensures scalability, reliability and cost-effectiveness.

**Figure 1-1 OCSM Architecture**




The architecture has three layers:

- The Probe layer captures network traffic and performs Media Quality analysis.
- The Mediation Engine (ME) layer correlates network traffic and stores it for future reference. This layer also measures, manages and stores the KPIs. While there is usually one ME per geographic site, one site may have multiple MEs or probes from multiple geographical sites may send traffic to a single ME.
- The Aggregation Engine (AE) layer aggregates the global KPIs, with on-demand call correlation and global search features. In a typical setup, there is only one AE for the whole network.

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 1-2 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 1-2 Fraud Monitor Login Page**


# 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.

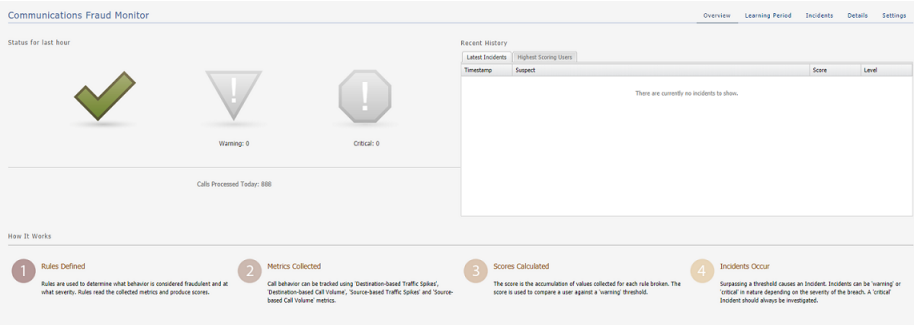
The Details page shows a single user and his incidents. This page contains a short history of the potential fraud that might have occurred.

# 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 1-3 shows the Overview page.

**Figure 1-3 Overview Page**




## 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.

# Learning Period Page

The **Learning Period** page displays information learned over time by Fraud Monitor.

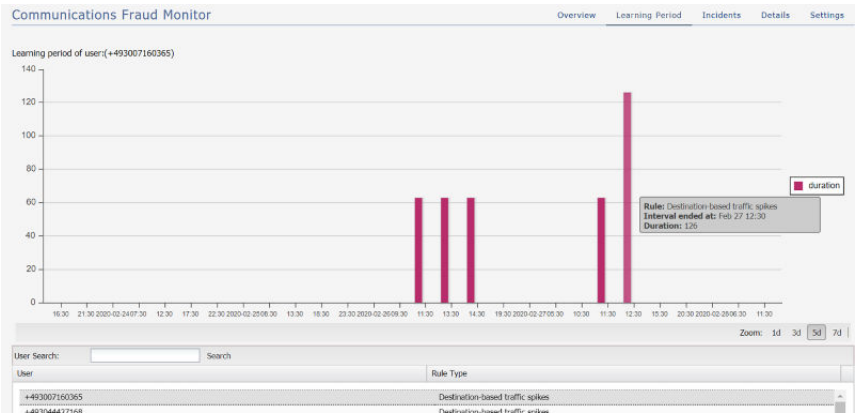
### Accessing the Learning Period Page

You can access the **Learning Period** page using the Learning Period link on the Fraud Monitor Home Page.

The **Learning Period** page is visible only to Admin users and displays user information for the following dynamic rules:

- Destination-based call volume
- Destination-based traffic spikes
- Source-based traffic spikes
- Source-based call volume

**Figure 1-4 User Listing on the Learning Period Page**




You can view 50 users last seen by the Fraud Monitor, and search dynamically learned user data for specific users. For each selected user, Fraud Monitor displays 7 days of previously captured user activities.

# Searching for Users in the Learning Period Page

The Learning Period Page displays user information and metric type rules.

To search for a user:

1. In the **Learning Period** page, type the user name in the **User Search** box. For example, 98765332333.

2. Click **Search**.

   The search results displays all such users that exactly match the query, and also a count of the all matches in shown.

> **Note:**
>
> The **User Listing** section displays data relevant for the last 7 days only.

## Viewing the Learning Period Graph

You can view the Learning Period graph for a specific user.

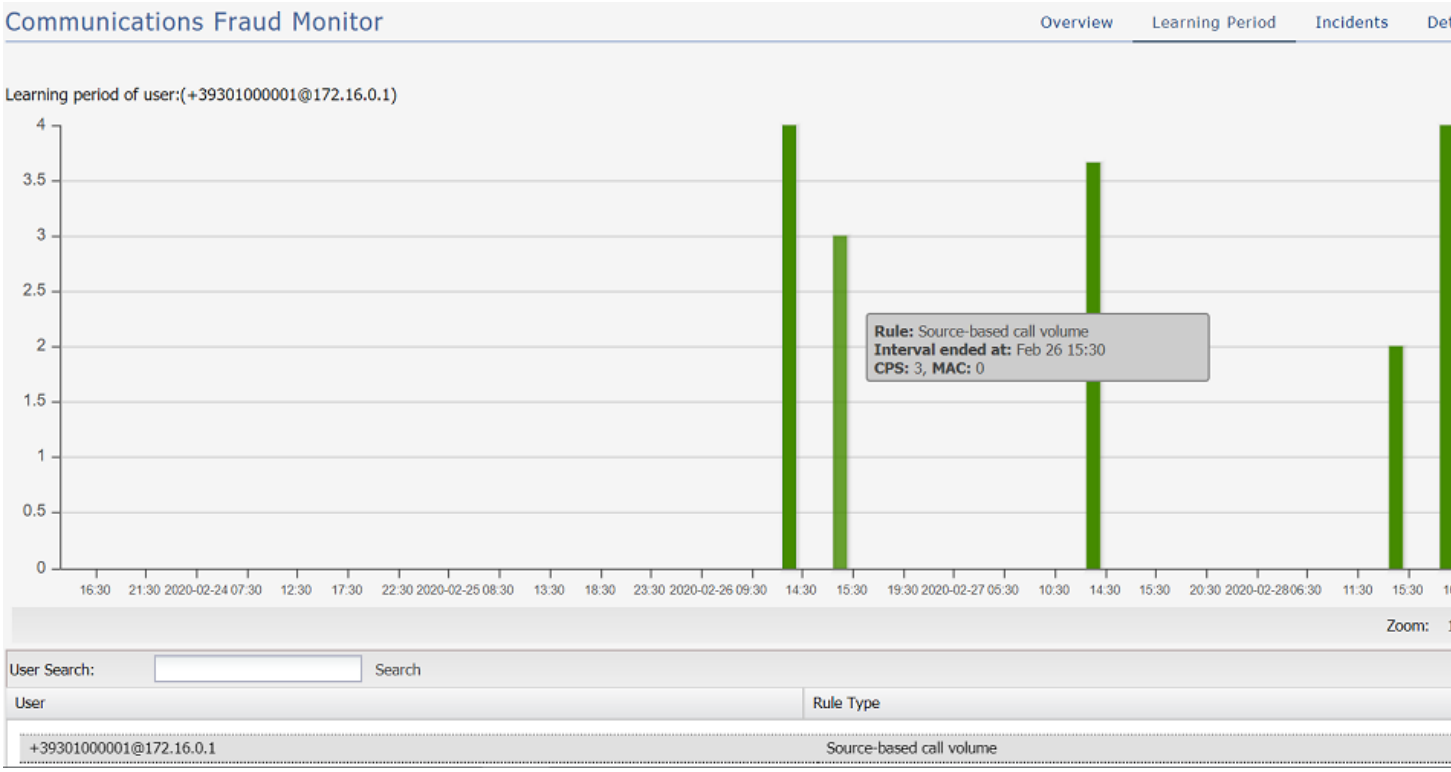
To view the graph:

1. Select a user from the **User Listing** section.

   The Learning Period graph is shown in first section of the page.

   - The X-axis of the graph shows time in hours.
   - The Y-axis of the graph displays the average duration of the call for destination-based-traffic-spikes and source-based-traffic-spikes. For source-based-call-volume and destination-based-call-volume the graph displays average calls per second and maximum active calls.

**Figure 1-5 Learning Period graph**




2. To adjust the period reflected in the graph, use the controls at the bottom of the graph.

# Incidents Page

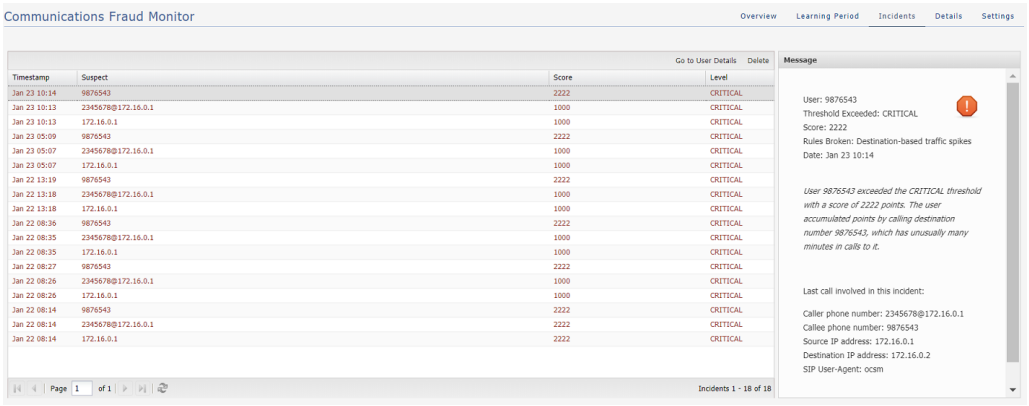
The Incidents page lists all the calls which have triggered incidents. This includes warning and critical incidents. See the Settings page to configure incident levels. As incidents are triggered they are added to the Incidents page in real-time.

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 1-6 Incidents Page**




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

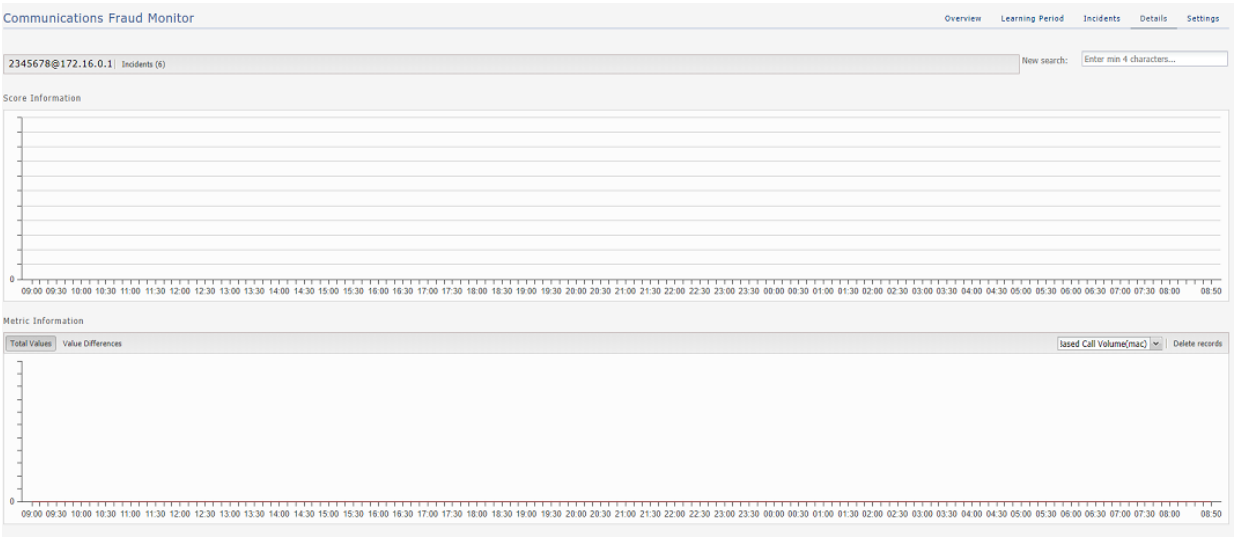
The Details page shows information on a particular user. Also, the whitelist for countries of this user can be maintained on this page and all records associated with this user may be deleted.

Figure 1-7 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 1-7 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

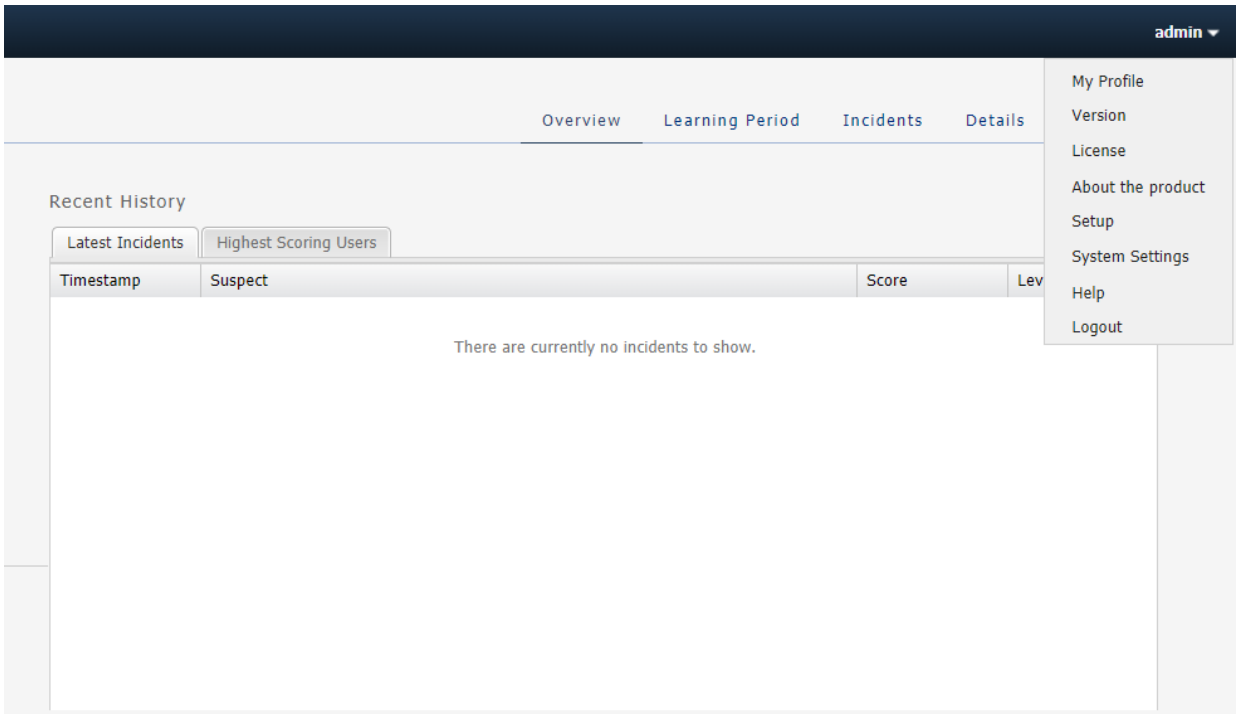
The alternative display modes in the top left corner, **Total Values** and **Value Differences**, toggle between displaying the current values as absolute values and as the difference to the average.

# 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 1-8 shows the User menu.

**Figure 1-8 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.

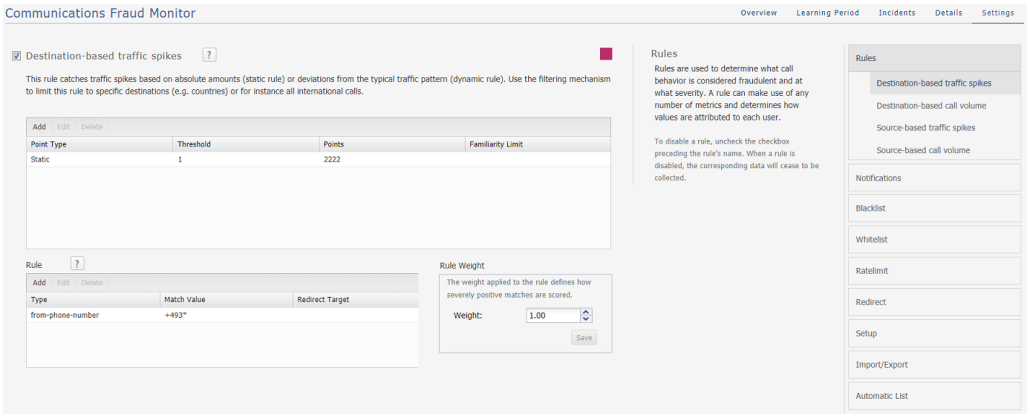
## Logging Out

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.



# 2
# 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.

# Rules in Fraud Monitor

Fraud Monitor uses rules to detect fraudulent calls. A rule uses multiple metrics and define how values are attributed to each user. Fraud Monitor provides four rules:

- Destination-based traffic spikes
- Destination-based call volume
- Source-based traffic spikes
- Source-based call volume

## Destination-based Traffic Spikes

This rule monitors traffic spikes based on absolute amounts (static rule) or deviations from the typical traffic pattern (dynamic rule).

The destination-based traffic spikes rule can be used to detect fraudulent calls based on traffic spikes. This rule is based on the threshold calculated on the basis of call duration (in minutes). If the parameters of the call match the parameters configured in the rule filter, and if the threshold is crossed, then the destination user of the particular call accumulates points. Once the user-accumulated points cross the threshold, an incident is raised, and an alert is sent to the user by email or SNMP.

In order to receive an email or SNMP notification, the email recipient or SNMP notification must be configured. For more information, see Setting Up Email Notifications.

## Destination-based Call Volume

This rule monitors destination traffic spikes based on deviations of Calls per Second (CPS) and Maximum Active Calls (MAC) from a typical traffic pattern (static and dynamic rule).

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.

Once the user-accumulated points cross the threshold, an incident is raised, and an alert is sent to the user by email or SNMP. To receive an email or SNMP notification, the email recipient or SNMP notification must be configured. For more information, see Setting Up Email Notifications.
This rule can be used to identify possible candidates for blacklisting or redirecting destination numbers.

## Source-based Traffic Spikes

This rule monitors traffic spikes based on absolute amounts (static rule) or deviations from the typical traffic pattern (dynamic rule). Fraud Monitor can raise an incident if a specific source

user generates unusually high traffic measured by call duration. If a threshold is exceeded, both the source and destination users accumulate points. This rule can be used to identify possible candidates for blacklisting source numbers.

The source-based traffic spikes rule is based on the threshold calculated on the basis of call duration (in minutes). If the parameters of the incoming call match the parameters configured in the rule filter, and if the threshold is crossed, then the source user of the particular call accumulates points. Once the user-accumulated points cross the notification threshold, an incident is raised, and an alert is sent to the user by email or SNMP. In order to receive an email or SNMP notification, the email recipient or SNMP notification must be configured. For more information, see Setting Up Email Notifications. You can define metric rules using call duration to measure the traffic spike.

## Source-based Call Volume

This rule monitors traffic spikes based on deviations of Calls per Second (CPS) and Maximum Active Calls (MAC) from the typical traffic pattern (static and dynamic rule).

Fraud Monitor can raise an incident if a specific source user generates unusually high call volume. If a threshold is exceeded, both the source and destination users accumulate points. This rule can be used to identify possible candidates for blacklisting source numbers. The source-based call volume rule is based on the threshold that is calculated on the number of calls per second and the maximum number of active calls. If the parameters of an incoming call match the parameters configured in the rule filter, and if a configurable threshold is crossed, then the source user for that particular call accumulates the point. Once the user-accumulated points cross the notification threshold level, an incident is raised and an alert is sent by email or SNMP. For more information, see Setting Up Email Notifications. In order to receive an email or SNMP notification, the email recipient or SNMP notification must be configured.

# 3
# 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.

# 4
# 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.

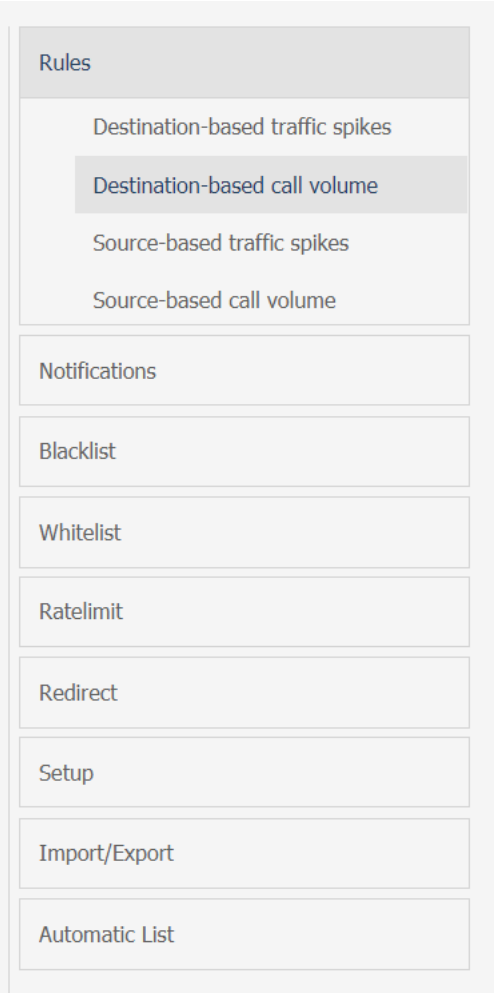
## Configuring Rules

Fraud Monitor 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.

To configure metric rules:

1. Click the navigation bar on the right-hand side of the page that lists the set of rules you can use.

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

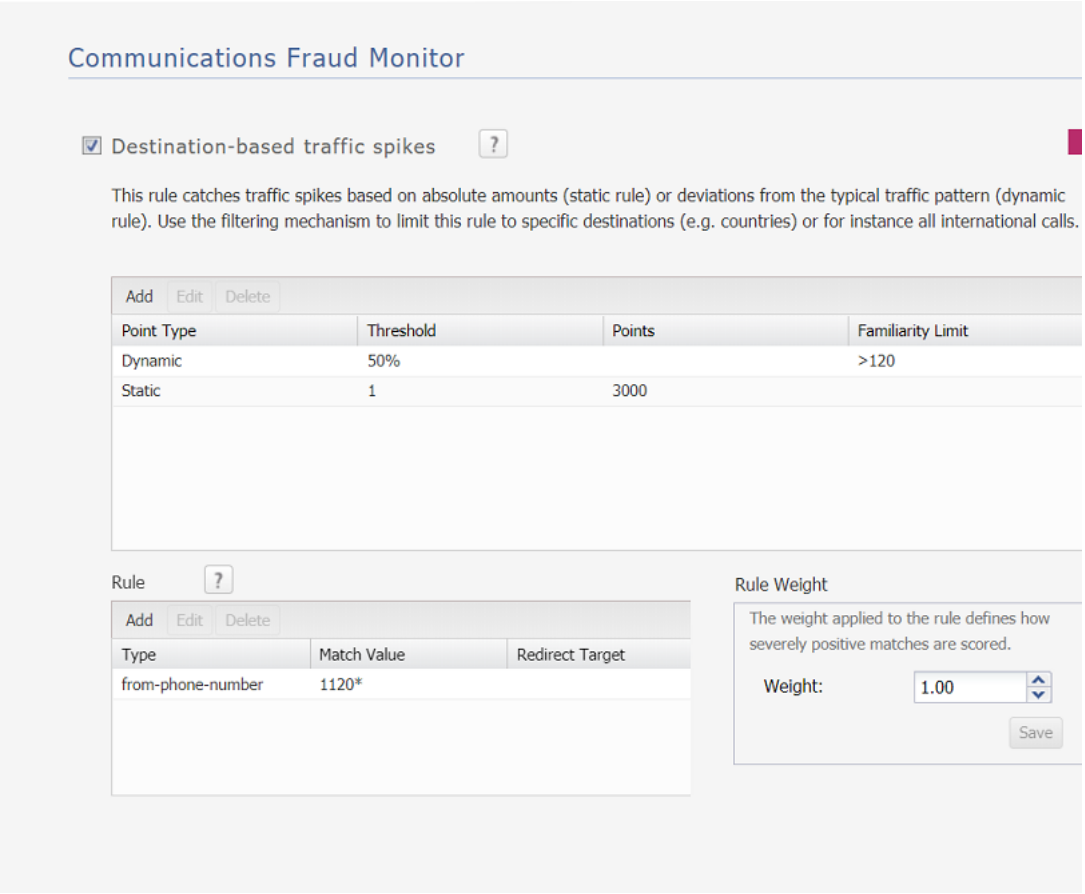



2. Click on a rule to open up its configuration panel in the left panel.

   Every configuration panel has **Add**, **Edit** and **Delete**, which you can use to configure a specific rule.

3. Use the check box next to the rule name in the left panel to enable or disable the rule. The check-box is enabled by default.

**Figure 4-2 Example of Rules Configuration**




4. Click **Add** to add the rule definition. The **Add Rule** window is displayed.
5. In the **Add Rule** window, define the rule using the threshold, point type, and Familiarity limits fields.

| Field | Description |
|---|---|
| Point Type | Select Dynamic or Static. For more information, see Configuring Points Accumulation. |
| Threshold | Threshold is the limit. If the threshold is crossed, then users accumulate points. Enter it in terms of percentage for a dynamic metric, or an integer for a static metric. |

| Field | Description |
|---|---|
| Familiarity limit | Familiarity is the difference in time relative to the time when the network user was seen by Fraud Monitor for the first time. Use the > or < prefixes to specify an upper or lower limit. For example, if you enter > 2, it means that a rule is only applicable if the user's timestamp is at least less than 2 hours in the past.<br>if you enter "<2", it means that a rule is only applicable if the timestamp for a given user is not yet 2 hours in the past.<br>If you do not specify the familiarity limit, then the rule is always applicable.<br>This is optional. |

6. Assign a **Rule Weight** The default is value **1.00**. The rule weight can be used to make some rules more important than others.

   Based on the Alert settings configured, if any user crosses the notification threshold on any rule, an incident is raised and a notification is sent to the user.

# Configuring Points Accumulation

Points are scores that a user accumulates when a threshold is crossed.

You can configure user points accumulation based on two methods:

- Dynamic
- Static

**Dynamic Method of Points Accumulation**

Dynamic points are the percentage points that a measured value deviates from a recorded average.

Total points is calculated as:

(((value - average) * 100) / average) * weight.

Dynamic points and percentage thresholds require a period of at least 24 hours for any user to compare a newly recorded value against a historic average. The minimum for the historical period is 24 hours.

**Static Method of Points Accumulation**

Users accumulate points if the call duration, or calls per second, or max active calls crosses the threshold value. You can configure the threshold in minutes for traffic spike rules. When the user crosses the threshold, points are assigned to the user. Points are calculated as:

Score = total points * weight.

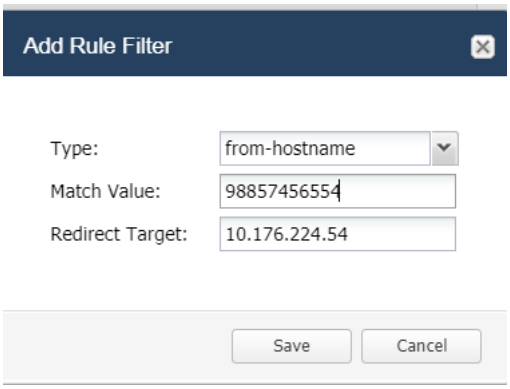
## Add Rule Filter

A rule filter is used to apply a rule to a subset of network calls. You can define a rule filter as regular expressions to filter calls based on phone numbers, Hostnames, Usernames, and User-agent headers.

To add a rule filter

1. In the window for configuring rules, click **Add**. For example, if you want to add rule filter for Source-based traffic spike rule, click **Add** in the Rule section. The **Add Rule Filter** window is displayed.

**Figure 4-3 Rule Filters**




2. Configure the rule filter using the Type, Match Value, and Redirect Target fields.

| Field | Description |
|---|---|
| Type | Lists the data type for the user. |
| Match Value | Use to specify the value for the Type selected above. For example, if you select the Type as from-phone-number, specify the phone number in the Match Value field. |
| Redirect Target | Add the IP address to which the call has to be redirected. This field is optional. |

3. Click **Save**.

# Setting Up Email Notifications

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

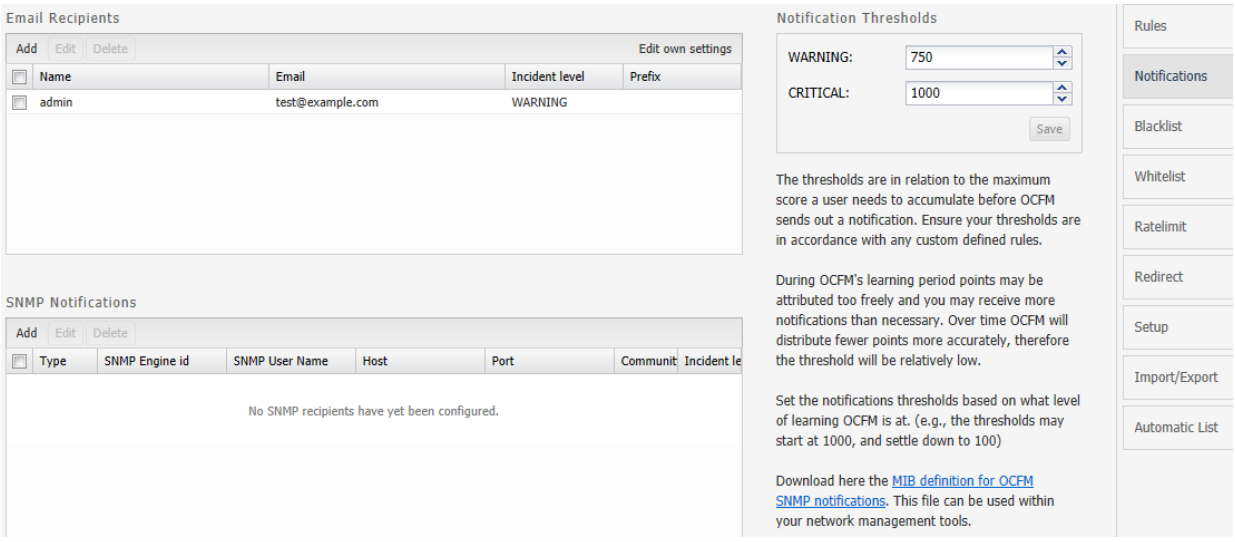
Figure 4-4 shows an example of the notification settings.

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
- **Expiry Updates**: If you select the **Receive Updates** option, then the information on expired subscribers from different lists is sent on the configured email address configured.

**Figure 4-4 Notification Settings for an Email Recipient**




# 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.

Using the **Configuration** menu option, you can:

- Enable and disable the Blacklist feature for specific data types.
- Configure the Expiry Timer Value. For more information, see Configuring the Expiry Timer

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.

You can configure the Expiry Timer Value using the Configuration menu. For more information, see Configuring the Expiry Timer.

# Specifying Ratelimit List

The Ratelimit list 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.
- Configure the Expiry Timer Value. For more information, see Configuring the Expiry Timer.

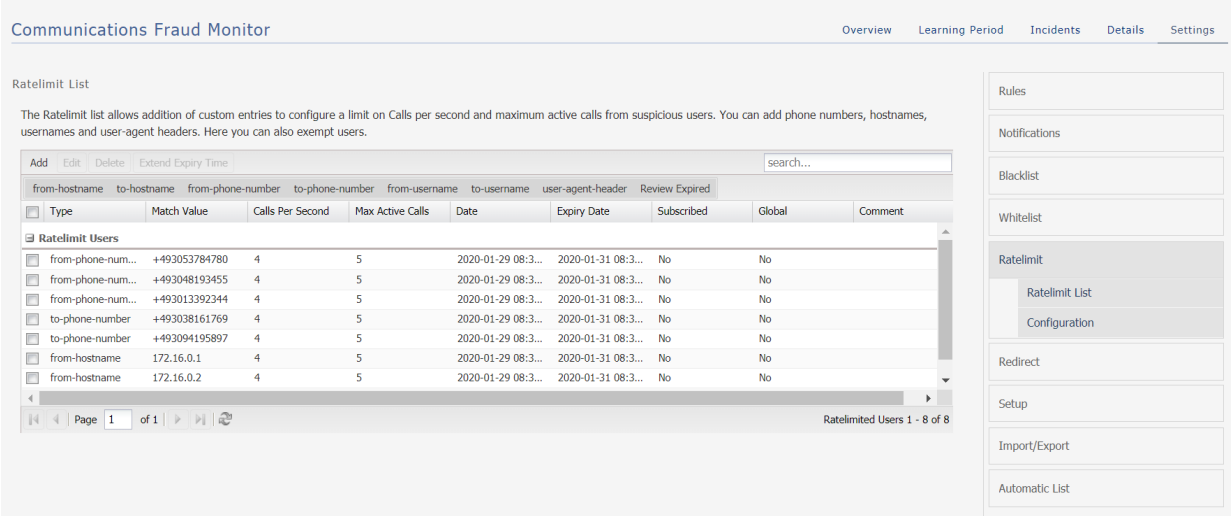
Should you want to exempt a specific entry, check the corresponding flag while adding or modifying that entry. But that exemption does not work for other lists like blacklist or redirect. If you want to exempt an entry from all lists, add the same in Whitelist. The CPS or MAC entries are not taken into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




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.

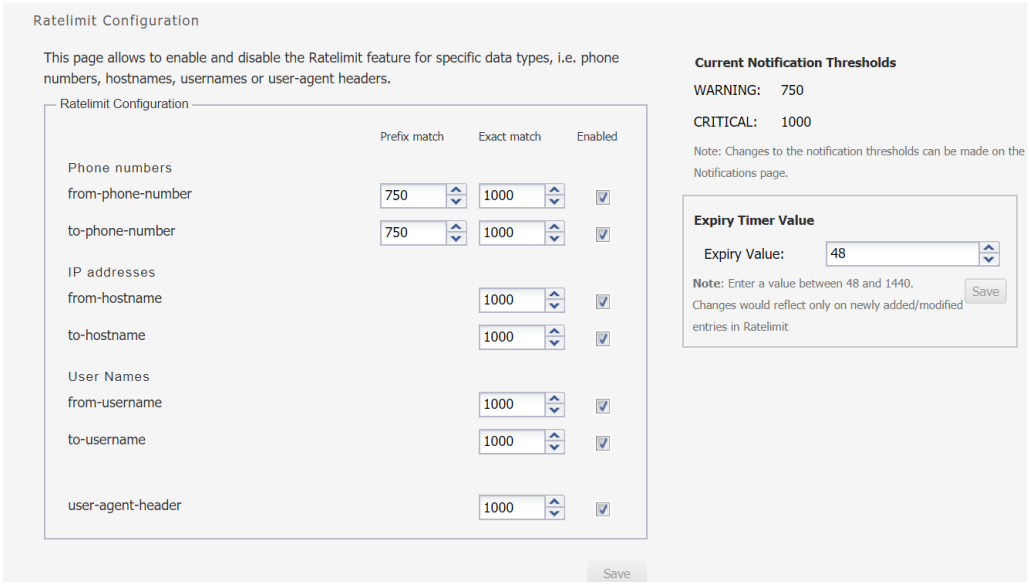
6. In the **Max Active Calls** field, enter the number of calls allowed for the user from the **Type** selected.
7. In the **Comment** field, enter any additional information for the user.
8. (Optional) Select **User exempted from ratelimit** to exempt from ratelimit.

> **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.




> **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.
- Configure the Expiry Timer Value. For more information, see Configuring the Expiry Timer.

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.

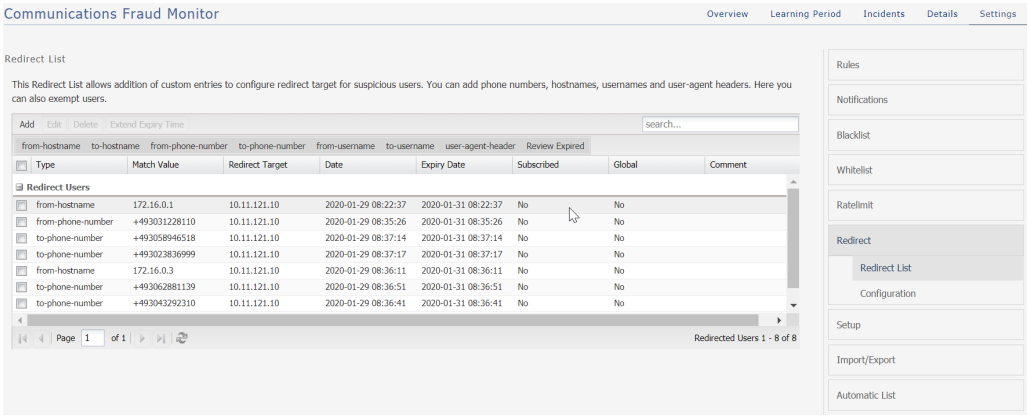
The Redirect supports all the data types supported by SBC for processing the calls. The available data type are:

- 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 4-5 Redirect List**




# 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, f**rom-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.

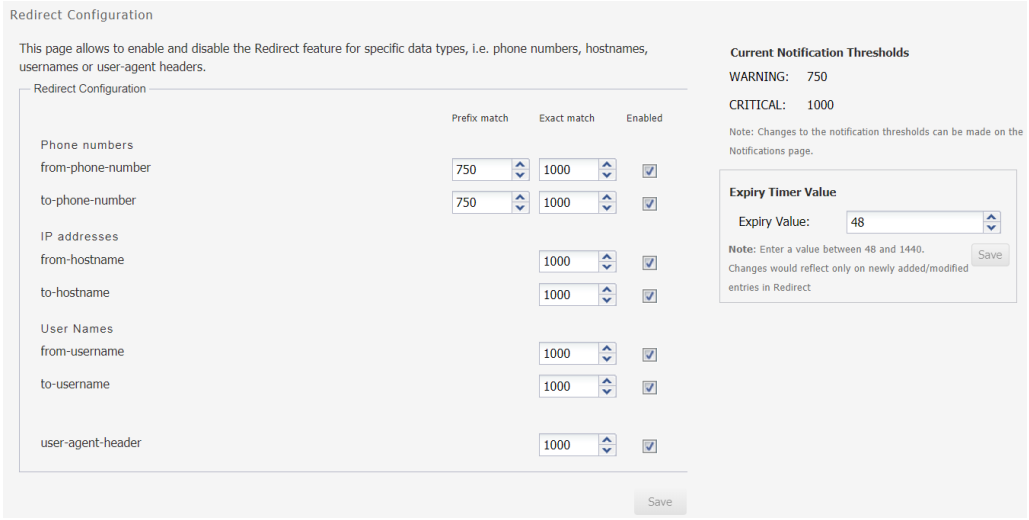
7. (Optional) Select **User exempted from redirect** to exempt from redirect.

   > **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.

8. 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.




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

# Automatic Deletion of Expired Entries

Fraud Monitor allows you to create various types of subscriber lists such as Blacklist, Whitelist, Ratelimit, and Redirect. A default expiry time of 48 hours is assigned to every subscriber entry in the lists.

A subscriber entry expires 48 hours after its addition to a list. A warning or notification in the form of an email/SNMP trap is sent out at 03:23 everyday.

If the administrator has enabled **System Settings** > **Automatic Expiry Delete**, then 24 hours after the expiry, all subscriber entries that have expired are deleted from the specific list. If you have not enabled the **Automatic Expiry Delete**, then as the administrator user, you can review the expired entries and delete them manually.

## Configuring Automatic Expiry Delete

The **Automatic Expiry Delete** option enables the automatic deletion of the expired entries in the Whitelist, Blacklist, Ratelimit, or Redirect lists. The expired subscriber entry is automatically deleted 24 hours after it's expiry.

To configure Automatic Expiry Delete:

1. Navigate to **admin** > **System Settings**.
2. In the **System Settings** dialog box, double-click **Automatic Expiry Delete**.
3. In the **Update System Setting** dialog box, select **Enabled** to enable the Automatic Expiry Delete setting. By default, it is disabled. If **Automatic Expiry Delete** is not enabled, then after the expiry, the entries are moved to the **Review Expired** tab, where you can manually review, delete or extend the expiry time.

# Applying Automatic Expiry for Existing Entries

You can set the expiry time for the existing subscribers of the previous release. If not enabled the existing entries will have the expiry date set as none. This action can be performed allowed only once.

To reset the expiry time of subscribers in all lists:

1. Click **admin** > **System Settings**.
2. In the **System Settings** dialog box, double-click **Apply Automatic Expiry for Existing Entries**.

   Doing so resets the expiry time of the existing subscriber entries of all lists. This feature impacts the Fraud Monitor performance.

# Configuring the Expiry Timer

You can configure the Expiry Timer Value which determines the expiry of a subscriber entry, and the deletion of the expired entries from the Whitelist, Blacklist, Ratelimit, and Redirect lists.

To configure the Expiry Timer Value:

1. Navigate to the required list for which the timer needs to be configured. For example, if you want to configure the timer for the Blacklist, go to: **Settings** > **Blacklist** > **Configuration**.

   You can configure the expiry time for each list separately. Subscribers of a list expire based on the Expiry Timer configuration of the list.
2. In the **Expiry Timer Value** section, add the value in terms of hours. The default value is 48 hours. This means that a subscriber entry expires 48 hours after its addition to the list. You can specify any value between 48 -1440 hours.

   A warning or notification in the form of an email/SNMP trap is sent out at 03:23 everyday. This notification contains a list expired subscribers. If you have enabled **admin** > **System Settings** > **Automatic Expiry Delete** , then 24 hours after the expiry, all expired entries are deleted from the list. If you have not enabled the Automatic Expiry Delete, the administrator can delete the expired entries from the list. This action cannot be performed by a non-admin user. For more information on enabling or disabling the Automatic Expiry Delete setting, see Configuring Automatic Expiry Delete.

# Reviewing and Extending the Expiry Time of Expired Entries

You can review the expired entries of a list, and extend the expiry time of multiple expired entries.

To extend the expiry time of entries:

1. Navigate to the list. For example, **Settings** -> **Blacklist** -> **Custom Blacklist**.

2. Click **Review Expired**. For more information, see Information in the Review Expired Tab
3. Select the entries for which you need to extend the expiry time. You can a select a maximum of 20 entries at one time.
4. Click **Extend Expiry Time**.
5. In the **Extend Expiry** dialog box, click **Yes** to confirm.

   The expiry time for the entry is extended by the value configured in the **Expiry Timer Value**.

# Deleting Expired Subscriber Entries

You can review and delete the expired entries using the **Review Expired** tab,

To delete the expired entries:

1. Navigate to the list. For example, **Settings** -> **Blacklist** -> **Custom Blacklist**.
2. Click the **Review Expired** tab. For more information, see Information in the Review Expired Tab.

   You can view the expired entries in the deleted_entries_`mm-dd-yy` file that is created everyday with information on the expired entries. This file is available under the `/tmp/expired_entries/` folder.
3. Select the entries that you need to delete. You can a select a maximum of 20 entries at one time.
4. Click **Delete** .

   Only the Administrator can delete the expired entries.

# Viewing the Automatically Deleted Expired Entries

You can view all expired entries that were automatically deleted from Fraud Monitor.

### Accessing the File Containing the Deleted Entries

The automatically deleted expired entries are available under the `/tmp/expired_entries/` folder. A file with the format `deleted_entries_mm-dd-yy` is created everyday with the information of the expired list entries that were deleted that day.

This file contains information on data type, and subscriber information. For example, list of Expired Elements: from-hostname 1.1.1.1.

# Information in the Review Expired Tab

This table lists the columns displayed in the Review Expired tab.

### Information in the Review Expired Tab

**Table 4-1 Review Expired Tab**

| Column Name | Description |
|---|---|
| Type | Data type of the subscriber |
| Match Value | Predicate value of subscriber |

**Table 4-1 (Cont.) Review Expired Tab**

| Column Name | Description |
|---|---|
| Date | Date when the subscriber was added to the list. |
| Expiry Date | Expiry Date of the subscriber |
| Subscribed | Boolean value if the subscriber is an automatic list |
| Global | Boolean value if the subscriber has been uploaded as a part of import functionality. |
| Comment | Description |

## Setting Up Notifications for Expiry Updates

Fraud Monitor sends notifications (Email/SNMP) to the user when it detects expiry of subscriber entries. If you do not want to receive such notifications, you can configure this in the **Notifications** page.

To set up notifications for Expiry updates:

1. Navigate to **Settings** > **Notifications**.
2. In the **Email Recipients** section, click **Edit own Settings**. to add or edit settings.
3. In the **Add email recipient** window, click: .
   - **Do Not receive updates** to not receive notifications on the expiry of the entries.
   - **Receive updates** to receive notifications.
4. Click **Finish**.

This configures Fraud Monitor not to send or to send notifications on the expiry of subscriber entries.

# 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 for the Mediation Engine. See the Configuring Fraud Monitor chapter.

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.

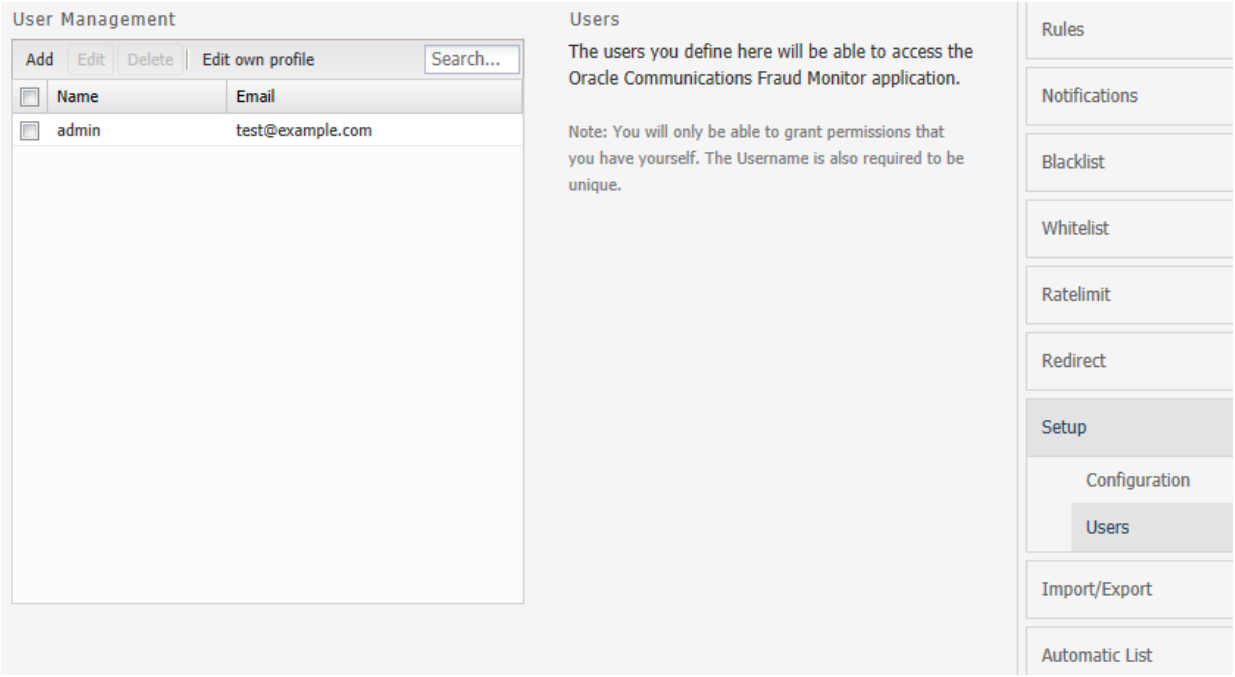
# Managing Users

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 4-6 shows an example of the users list.

**Figure 4-6 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**.

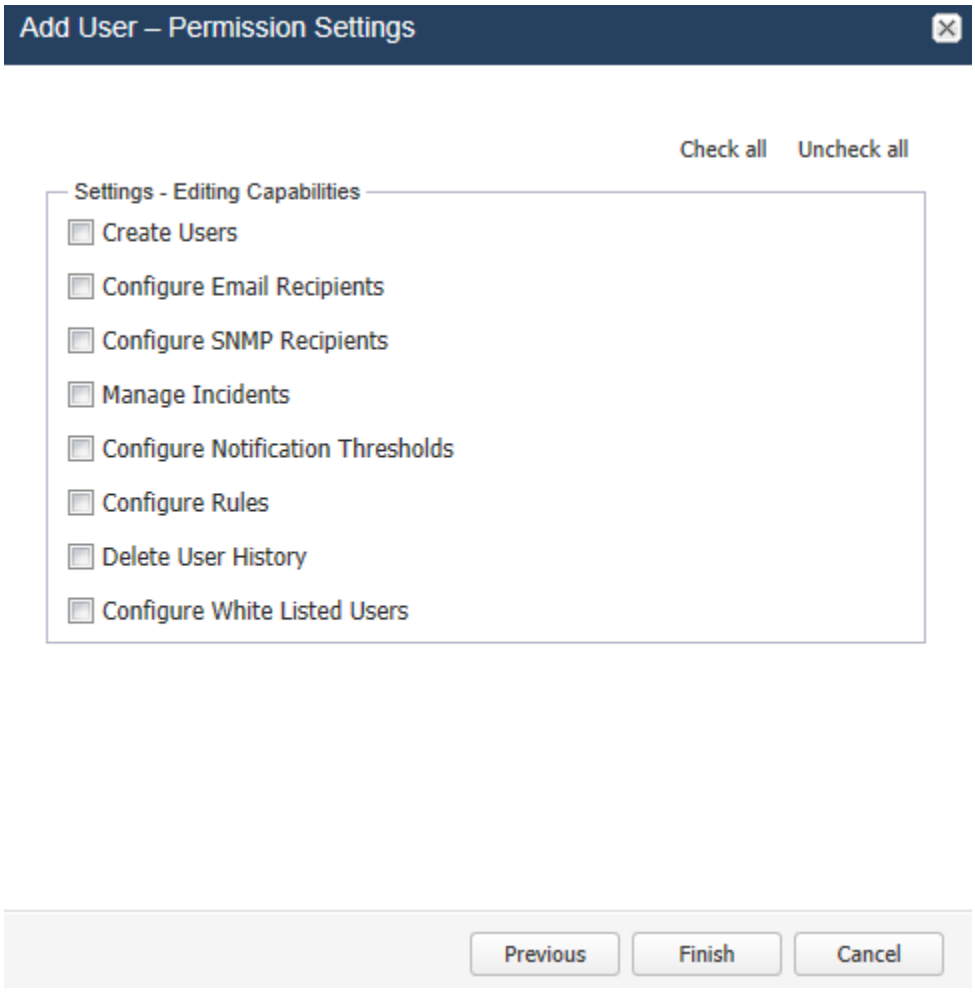
   The Add User - Permission Settings screen appears.
4. Select the permissions for the user by clicking the checkbox. Alternatively, you can click **check all** and **uncheck all** options.

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 4-7 shows the user permission settings.

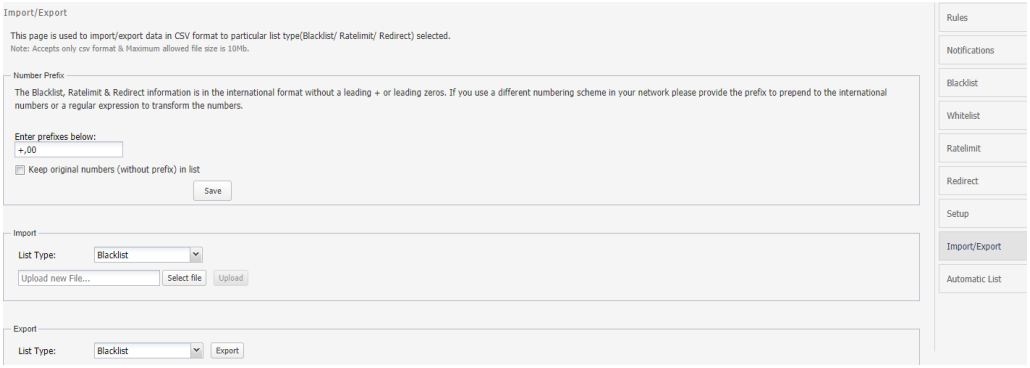
**Figure 4-7 Granting Capabilities to the New User**




# 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.




From this screen, you can:

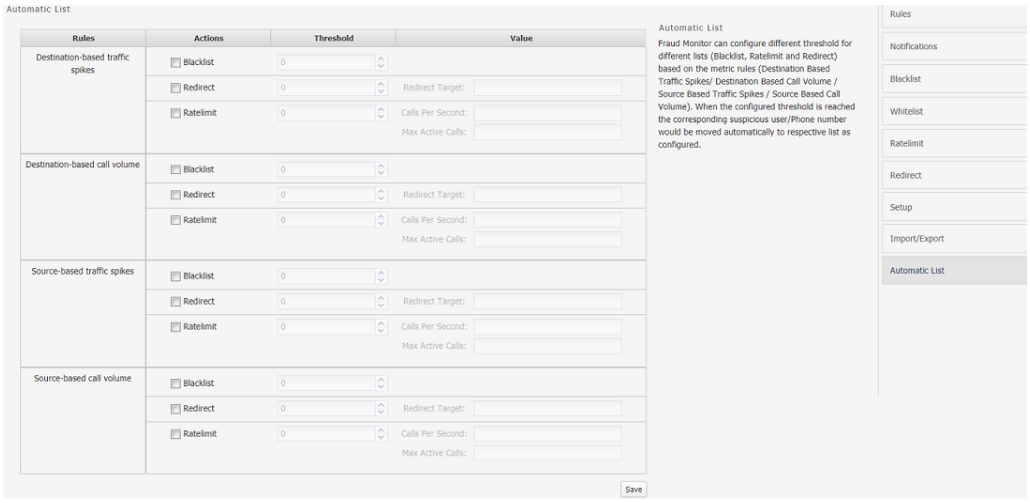
- **Number Prefix**: You can enter prefixes of the phone numbers to save the data for exporting and importing. The Blacklist information is in the international format without a leading + or leading zeros.

  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
Destination-based call volume
Source-based traffic spikes
Source-based call volume
Blacklist
Redirect
Ratelimit
Redirect Target:
Calls Per Second:
Max Active Calls:
Save
Automatic List
Fraud Monitor can configure different threshold for different lists (Blacklist, Ratelimit and Redirect) based on the metric rules (Destination Based Traffic Spikes/ Destination Based Call Volume / Source Based Traffic Spikes / Source Based Call Volume). When the configured threshold is reached the corresponding suspicous user/Phone number would be moved automatically to respective list as configured.
Rules
Notifications
Blacklist
Whitelist
Ratelimit
Redirect
Setup
Import/Export
Automatic List