

Oracle® Communications

Session Element Manager User Guide for the Enterprise Utilities Plug-in



Release 2.0
October 2018

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2017, 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.

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

1 Overview

Session Element Manager Parts	1-1
Session Element Manager Prerequisites	1-2
Information for Oracle Enterprise Operations Monitor Users	1-2
Information for Oracle Interactive Session Recorder Users	1-3

2 Device Manager

Configure Device Groups	2-1
Using the Default Home Device Group	2-2
Add a Device Group	2-2
Move a Device Group to Another Device Group	2-3
Rename a Device Group	2-3
Delete a Device Group	2-3
Manage Network Functions and Devices	2-4
Oracle Enterprise Utilities Plug-in Product Category and Network Function Types	2-4
Add a Network Function with Devices	2-4
Manage Network Functions	2-5
Launch a Managed Device Login Page	2-5
Edit a Network Function with Devices	2-5
Move a Network Function to Another Group	2-6
Lock or Unlock a Network Function	2-6
Override a Locked Network Function	2-6
Override a Locked Device	2-7
View Network Function Information	2-7
View Device States and Columns	2-7
Manage How Groups for Network Functions are Displayed	2-9
View Serial Numbers for a Physical Device	2-9
Export Device Information from Device Manager	2-9
Export Detailed Device Information from Device Manager	2-10

3 Fraud Protection Manager

Fraud Protection Manager Search Filters	3-2
Configure a Fraud Detection and Prevention Device Registration	3-2
Add a Fraud Detection and Prevention Device Registration	3-2
Register a Fraud Detection and Prevention Device	3-4
Re-register a Fraud Detection and Prevention Device	3-4
Edit a Fraud Detection and Prevention Device Registration	3-5
View Fraud Detection and Prevention Device Registration Information	3-5
Search Fraud Detection and Prevention Device Registrations	3-6
Re-synchronize Session Delivery Manager with Fraud Protection List Data	3-7
Unregister a Fraud Detection and Prevention Device	3-7
Register a Fraud Detection and Prevention Device	3-7
Delete a Fraud Detection and Prevention Device Registration	3-8
About Fraud Protection Lists	3-8
Fraud Protection List Type Entries	3-8
Fraud Protection List Data Types	3-9
Fraud Protection List Data Type Formats	3-9
Configure Fraud Protection Lists	3-9
Add a Fraud Protection List	3-10
Add a Fraud Protection List Entry	3-10
Import a Fraud Protection List	3-11
Upload a Fraud Protection List from a Device	3-12
Copy Fraud Protection List Contents to Another Fraud Protection List	3-12
Assign Fraud Detection and Prevention Device to a Fraud Protection List	3-13
Unassign Fraud Detection and Prevention Device to a Fraud Protection List	3-13
Manage Fraud Protection Lists	3-14
Edit a Fraud Protection List	3-14
Manage a Fraud Protection List Entry	3-14
Edit a Fraud Protection List Entry	3-15
Copy a Fraud Protection List Entry	3-16
View Fraud Protection List Entry Information	3-17
Search Fraud Protection List Entry Information	3-17
Delete a Fraud Protection List Entry	3-18
Unassign a Fraud Detection and Prevention Device from a Fraud Protection List	3-18
View Fraud Protection List Information	3-19
Search for a Fraud Protection List	3-19
Delete a Fraud Protection List	3-20
Configure Fraud Protection List Push Task Updates	3-21
Add a Fraud Protection List Push Task	3-21
Manage Fraud Protection Push Task Updates	3-23

Edit a Fraud Protection List Push Task	3-23
Commit a Fraud Protection List Push Task Manually	3-25
Update Fraud Protection List Changes Manually When Automatic Updates are Enabled	3-25
Stop Fraud Protection List Push Task Updates	3-25
Copy a Fraud Protection List Push Task	3-26
Resubmit a Device Group Push Task	3-26
View Fraud Protection List Push Task Information	3-26
View Device Group Push Tasks	3-28
Search for a Fraud Protection List Push Task	3-29
Delete a Fraud Protection List Push Task	3-31
Configure a Fraud Protection List Backup Schedule	3-31
Add a Fraud Protection List Backup Schedule	3-31
Manage the Fraud Protection List Archive	3-32
Edit a Fraud Protection List Backup Schedule	3-32
Backup a Fraud Protection List Now	3-33
Restore a Fraud Protection List Backup	3-33
View the Fraud Protection List Backup Schedule	3-33
Search the Fraud Protection List Archive	3-34
Delete a Fraud Protection List Backup Schedule	3-34
Configure Fraud Protection List Purge Policies	3-34
Create a Fraud Protection List Purge Policy	3-35
Purge Fraud Protection Lists On-Demand	3-35

About This Guide

This document and other product-related documents are described in the Related Documentation table.

Oracle 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>.

Related Documentation

Table Oracle Communications Product Plug-in Documentation Library

Document Name	Description
Session Element Manager User Guide	Provides information for managing and optimizing network infrastructure elements and their functions with comprehensive tools and applications used to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed network functions and their associated devices in Oracle Communications Session Delivery Manager (SDM).
Report Manager User Guide	Provides information about configuring Report Manager to interoperate with Oracle BI Publisher as well as creating reports on Session Delivery product network devices.
Report Manager Installation Guide	Provides information for installing Oracle Communications Report Manager product as an addition to SDM including the Oracle database and BI Publisher components. The Oracle session delivery product plugin must be added to Oracle Communications Session Delivery Manager before performing the Report Manager installation.
Route Manager User Guide	Provides information for updating local route table (LRT) data on a single device or multiple devices.

Table Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	<p>Provides the following administration information:</p> <ul style="list-style-type: none">• Implement SDM on your network as a standalone server or high availability (HA) server.• Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password.• Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed.• Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices.• Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems.• Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics.• Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations.• Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	<p>Provides the following installation information:</p> <ul style="list-style-type: none">• Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons.• Do the typical installation to perform the minimal configuration required to run the SDM server.• Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.
Release Notes	<p>Contains information about the administration and software configuration of the SDM feature support new to this release.</p>
Security Guide	<p>Provides the following security guidelines:</p> <ul style="list-style-type: none">• Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines.• Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system.• Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	<p>Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.</p>
SOAP API Guide	<p>The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programming model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.</p>

Revision History

Date	Description
July 2018	<ul style="list-style-type: none">Initial release
September 2018	<ul style="list-style-type: none">With the introduction of the Enterprise Utilities Plug-in Release 2.1, a Fraud Detection and Prevention (FDP) device is now supported.
October 2018	<ul style="list-style-type: none">Adds the "Fraud Protection Manager" chapter.Adds conceptual information to "Oracle Enterprise Utilities Plug-in Product Category and Network Function Types" regarding OCSEM's use of Network Functions (NFs).

1

Overview

Oracle Communications Session Element Manager is used to manage and optimize network infrastructure elements and their functions with comprehensive tools and applications on Oracle Communications Session Delivery Manager to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed devices.

Session Element Manager Parts



Data Variables

Data variables (DVs) are used in offline configurations to allow network administrators to target elements that require device-specific information. All data variables must have new values to push the configuration to a device. An offline configuration requires DVs that have different values for each device that the template is assigned to support. This allows the template to be finely adjusted to the specific needs of a device and continue to provide a common baseline configuration for many devices. The template editor allows you to apply data variables to any element attribute that the offline configuration supports. A derived value can be specified when the DV that you are configuring shares the same value as another DV (dependency).

Device

A device is the atomic object that cannot be sub-divided and represents the component that does the required work. The element manager supports a network function (NF), but also manages the devices the NF contains.

Device group

A device group can contain or group NFs and devices.

Element Manager

The Oracle Communications Session Element Manager (SEM) provides alarm, configuration, fault, loading and provisioning capabilities for devices, performance management for infrastructure elements, and security capabilities.

Geo-redundant group

A geo-redundant group has active and standby devices that are not co-located.

Network Element

A network element is a manageable logical entity uniting one or more physical devices.

Network Function

An NF can be composed of device groups and devices. An NF can be simple or complex. A simple NF can be a standalone device or a high-availability (HA) pair. A complex NF can consist of device groups that further define topological constructs and complex structures for device containment.

Session Element Manager Prerequisites

The following prerequisites are required before you can access product plugin FCAPS functionality in the Session Delivery Manager GUI.

 **Note:**

Unsupported features are hidden or disabled by the product plugin.

- You must install the Session Delivery Manager server before you can install your product plugin through the Session Delivery Manager GUI. See the *Oracle Communications Session Delivery Manager Installation Guide, Release 8.1* for Session Delivery Manager server installation instructions.
- You must upload and install the product plugin in the Session Delivery Manager GUI. See the *Session Delivery Manager Software Distribution Media* section in the *Oracle Communications Session Delivery Manager Release Notes, Release 8.1* for the file name of your product plugin, and the *Oracle Communications Session Delivery Manager Administration Guide* for product plugin upload and installation instructions.

Information for Oracle Enterprise Operations Monitor Users

The Oracle Communications Session Element Manager (OCSEM) Enterprise Utilities plug-in supports using the Oracle Enterprise Operations Monitor (EOM) with the **Device Manager** to add and manage devices and device groups. OCSEM does not support the EOM in any of the other sliders.

Once the Enterprise Utilities plug-in is installed, you can launch the EOM login page. You can add and manage devices in **Device Manager** with the following exceptions:

- OCSEM does not support applying work order administration to the EOM, even though a work order displays the EOM as a selection.
- OCSEM does not support the **Show Details** functionality for the EOM.

Note that the Managed Devices - Group View page in SEM displays the following additional controls for working with Enterprise Plug-ins.

- **Add**—Launch the SEM dialogs for adding Enterprise devices.
- **View**—View the selected Enterprise device.
- **Launch**—Launch the login page for the selected Enterprise device.

Refer to the *Device Manager* chapter for more information.

Information for Oracle Interactive Session Recorder Users

The Oracle Communications Session Element Manager (OCSEM) Enterprise Utilities plug-in supports using the Oracle Interactive Session Recorder (ISR) with the **Device Manager**. OCSEM does not support the ISR in any of the other sliders.

Once the Enterprise Utilities plug-in is installed, you can launch the ISR login page. You can add and manage devices in **Device Manager** with the following exceptions:

- OCSEM does not support applying work order administration to the ISR, even though a work order displays the ISR as a selection.
- OCSEM does not support the **Show Details** functionality for the ISR.

Note that the Managed Devices - Group View page in SEM displays the following additional controls for working with Enterprise Plug-ins.

- **Add**—Launch the SEM dialogs for adding Enterprise devices.
- **View**—View the selected Enterprise device.
- **Launch**—Launch the login page for the selected Enterprise device.

Refer to the *Device Manager* chapter for more information.

2

Device Manager

The **Device Manager** slider is used to create a grouping hierarchy and add one or more network functions (NFs) to this grouping schema.

You can assign individual devices to a network function (NF) group, which can contain a standalone device, high-availability (HA) pair, or device cluster that is managed by Oracle Communications Session Element Manager. Device groups can exist in a grouping hierarchy that can be set up to contain any number of levels according to the needs of your organization. For example, you can structure your hierarchy based on geography. User permissions can be managed based on operation and device group privileges. Summary and detailed information can be displayed for individual devices and device groups.

You can assign individual devices to a network function (NF) group, which can contain a standalone device or a high-availability (HA) pair that is managed by Oracle Communications Session Element Manager. Device groups can exist in a grouping hierarchy that can be set up to contain any number of levels according to the needs of your organization. For example, you can structure your hierarchy based on geography. User permissions can be managed based on operation and device group privileges. Summary and detailed information can be displayed for individual devices and device groups.

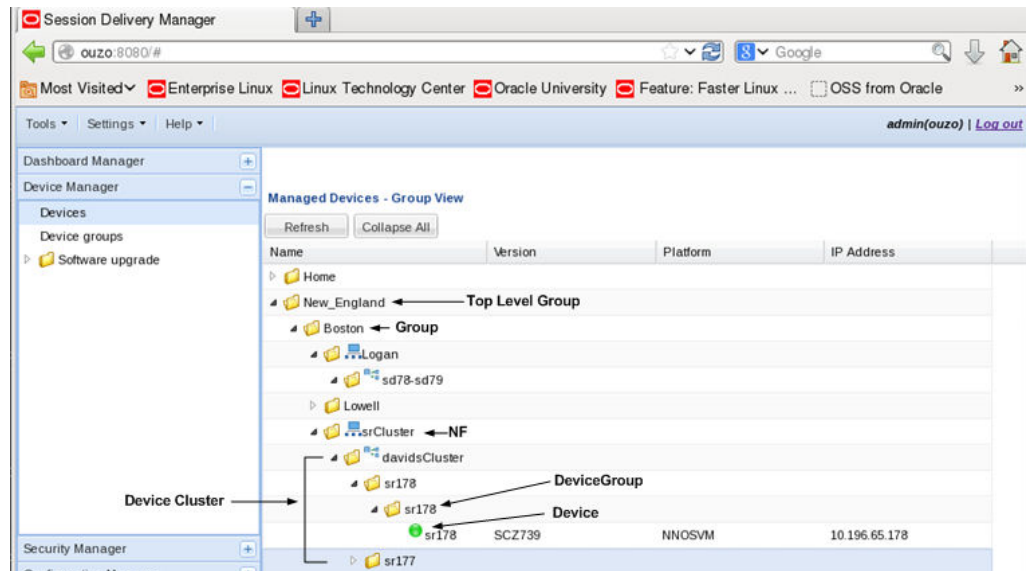
The **Device Manager** slider contains the following nodes and folder nodes:

- **Devices**—Add, manage, and remove managed devices.
- **Device Groups**—With the appropriate permissions, you can add, manage, rename, and remove groups.
- **Device Clusters**—Add, remove, and manage devices belonging to a cluster that share the same hardware, software, and configuration.

Configure Device Groups

You can configure a device group topology. One or more device groups can be nested to define the topology of the network, which can include naming conventions such as geographical references and location names. Once a device group is specified, user privileges must be assigned to the group appropriately. For example, if the user is only allowed to view the NF and its devices, then the privilege is set to **VIEW**. If the user is allowed to add or run commands on the NF and its devices, the privilege is set to **FULL**. See the *Security Manager* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* and the *Configure a Network Function for Devices* section later in this chapter for more information respectively.

Figure 2-1 Grouping Structure for a device cluster



Using the Default Home Device Group

You can add your NFs to the default **Home** device group if no other groups need to be created. Use this group with the following conditions:

- You must be assigned full administrative privileges to view this device group.
- You cannot rename this device group.
- You cannot delete this device group.
- When adding a device, the **Home** device group displays in the **Add device group** dialog box only if you have not targeted a previous device group from the table.

Add a Device Group

Use the following naming conventions when you add a device group:

- It must start with an alphabetic character.
- It can contain a minimum of three characters and a maximum of 50 characters.
- It can contain the following characters: alphabetic, numeric, hyphens (-), and underscores (_).
- It can be a mix of upper-case and lower-case characters.
- It cannot contain symbols or spaces.
- It cannot be the same name as an existing group name within the same level in the hierarchy (sibling).

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click **Add**.
3. In the **Add device group** dialog box, enter the name for the device group in the **Device group name** field and click **OK**.

The device group now appears in the **Device Groups** pane.

Move a Device Group to Another Device Group

When a device group is moved, all devices within that device group are moved.

Note:

A device group cannot be moved into one of its child groups.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click the device group you want to move and click **Admin, Move**.
3. In the **Move device group(s) to** dialog box, click the device group in which you want to move your device group and click **OK**.

Rename a Device Group

You can rename a device group if it does not belong to another device group at the same hierarchical level.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device groups** pane, select the device group you want to rename and click **Rename**.
3. In the **Rename device group** dialog box, enter the new name in the **Rename device group to** field and click **OK**.

The new name appears in the **Device Groups** pane.

Delete a Device Group

You can delete a device group (folder) from the **Device Groups** list with the appropriate permissions, and under the following conditions:

- Empty the device group folder and move all devices to another device group folder or delete the devices from the device group folder in order to delete the device group folder.
 - You cannot delete a device group if it causes a duplicate device group in the tree hierarchy.
1. Expand the **Device Manager** slider and click **Device Groups**.
 2. In the **Device Groups** pane, click the device group and click **Delete**.
 3. In the **Delete device group** confirmation dialog box, click **Yes** to delete the device group.
 4. In the success dialog box, click **OK**.

Manage Network Functions and Devices

Oracle Enterprise Utilities Plug-in Product Category and Network Function Types

As of Oracle Communications Session Element Manager Release 8.0, the previous device nodes (used in OCSEM 7.x) that maintained the standalone or HA pair devices were replaced with the concept of a Network Function (NF). NFs are a network architecture concept used to describe entire classes of network node functions into building blocks that may connect, or chain together, to create communication services as defined by the *GS NFV-MAN 001 - ETSI*. In this context, a NF can be composed of one-to-many Edge devices. For example, a SBC-based NF can be composed of two SBC instances running as a HA pair.

The following table describes the product category and Network Function (NF) types that you select for your Oracle Enterprise Utilities Plug-in.

Product Category	NF Type	Component Devices
Enterprise Utilities	EOM	Enterprise Operations Monitor (EOM) device
	ISR	Interactive Session Recorder (ISR) device
	FDP	Fraud Detection and Prevention (FDP) device

Add a Network Function with Devices

When preparing to use Device Manager, you set up device groups and add Network Functions (NF) to the groups. After you successfully add a NF, the system can communicate with the associated device and you can launch the login page for the device by way of the Session Element Manager.

- Optional—If you do not want to use the default device group, named Home, add the device group that you want. See "Configure Device Groups for Network Function."
- Configure SNMP community on each device that you plan to add to the device to Device Manager. See the device documentation.

Use the following procedure to add a Network Function (NF) to a managed device group. You can add more NFs by repeating the procedure.

Note:

The table in the following procedure displays all possible configuration attributes, but the system displays only the set that corresponds to the selections that you make in this configuration.

1. Expand the **Device Manager** slider, and click **Devices**.
2. In the **Managed Devices - Group View** pane, select a device group, and click **Add**.
3. In the **Select Network Function Type** dialog, do the following:

- a. Select a **Category** from the drop-down list.
 - b. Select a **Network Function** from the drop-down list.
4. Click **Continue**.
 5. In the **Add Network Function: Device** dialog, complete the following fields:

Network Function Name	Enter the NF name that you want to use for the device you are configuring.
IP address	Enter the IP address for this device.
Web Protocol	Select HTTP or HTTPS from the drop-down list.
Web Port	Enter the web port.

6. Click **Apply**.
The system adds the NF to the specified managed device group and displays a green icon by the name of the device in the Managed Devices - Group View table upon successful addition.

Manage Network Functions

Once you have added one or more NFs with a group hierarchy, you can manage them as described in the following sections.

Launch a Managed Device Login Page

You can use Oracle Communications Session Element Manager as a single source from which to access and manage multiple products. When you select a device and click **Launch**, the system communicates to the device and displays the login page.

1. Expand the **Device Manager** slider, and click **Devices**.
2. On the **Managed Devices - Group View** page, select the device that you want to login to.
3. Click **Launch**.

The system displays the login page for the selected device.

Edit a Network Function with Devices

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, expand the appropriate group folder hierarchy, select the NF folder and click **Edit**.
3. In the **Edit device group** dialog box, change the appropriate parameters:

Network Function Name field	(Read-only) The NF name.
IP address field	(Read-only) The IP address for this device.
Web protocols	Select the web protocol from the drop-down list.
Web port	Enter the web port.

4. Click **Apply**.

A success dialog box displays that the NF was changed.

Move a Network Function to Another Group

You cannot move the NF if it is locked unless you are the owner of the lock or an administrator overrides the lock. An error message appears in both situations. See [Override a Locked Network Function](#) section for more information about unlocking an NF.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** page, expand the appropriate group folder hierarchy, select the NF folder and click **Admin, Move**.
3. In the **Move Device** dialog box, click the device group folder to which you want to move the NF and click **OK**.
4. In the **Success** dialog box, click **OK**.

The NF moves to the new folder location that you specified.

Lock or Unlock a Network Function

You can lock or unlock an NF and its device(s) with the appropriate administrator permissions.

Note:

Other users are prevented from rebooting, updating or modifying the configuration or route sets for an NF when you lock it. Only users with granted override lock permissions can override your lock or the NF must be unlocked by you.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the NF you want to lock and click **Admin, Lock** if it is unlocked or **Admin, Unlock** if it is locked.
3. In the confirmation dialog box, click **Yes**.

A padlock icon appears next to the IP address of the NF folder and its device(s). This padlock is removed if the NF is unlocked.

Override a Locked Network Function

Note:

You must have the appropriate privileges assigned by your administrator to override a lock set on an NF by another user.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the NF folder icon you want to override lock and click **Admin**.
3. From the **Admin** pop-up menu, select **Override lock**.
4. In the **Confirm** dialog box, click **Yes**.

5. In the **Managed Devices** pane, click **Refresh**.

The padlock icon no longer appears next to the NF folder and IP address(es) of the device(s).

Override a Locked Device

Note:

You must have the appropriate privileges assigned by your administrator to override a lock set on a device by another user.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, expand the NF folder and select the device that you want to override lock and click **Admin**.
3. From the **Admin** pop-up menu, select **Override lock on device**.
4. In the **Confirm** dialog box, click **Yes**.
5. In the **Managed Devices** pane, click **Refresh**.

The padlock icon no longer appears next to the device.

View Network Function Information

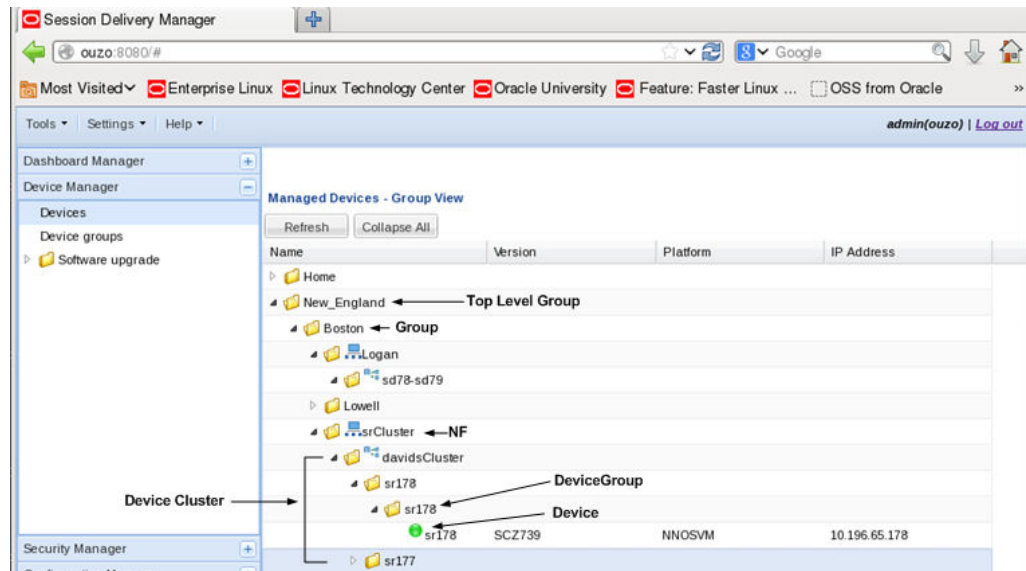
Use the following sections to view and manage Oracle session delivery product NF information, which includes its devices and the way detailed and summary NF information is displayed for its device node(s).

View Device States and Columns

You can monitor a variety of information for devices by viewing the state of their colored, round icons, and by using the column information presented for each device.

Expand the **Device Manager** slider and click **Devices**. The system displays a device group hierarchy showing the group, subgroup, and the network function (NF) that contains the devices, as shown in the following example.

Figure 2-2 Device groups and their associated NF devices



The following states of a device in the **Managed Devices** table indicate if it can be reached by Oracle Communications Session Element Manager:

- Green—The Oracle Communications Session Element Manager can reach the device and retrieve information about the device through SNMP.
- Red—The Oracle Communications Session Element Manager cannot currently reach the device (or cannot contact both devices in an HA device pair).

The following columns appear in the **Managed Devices** table:

Name	The group, subgroup, network function (NF) and device that belong to each NF. The grouping structure of the NF and its device is determined by the Session Delivery plug-in.
Version	The full software release version, including patch number of the NF HA device pair or standalone device.
Platform	The device hardware platform.
IP Address	The device IP address.
Serial Number	(Hidden) Serial number of the standalone device or the primary device in an HA deployment.
Group ID	(Hidden) The group element ID.
Object ID	(Hidden) Internal database object ID.
Offline Configuration	(Hidden) The name of the offline configuration associated with a specified NF device cluster.
Synchronized Mode	(Hidden) This column describes when Synchronized Mode is enabled or disabled for a specified NF device cluster.
ScalabilityGroupId	(Hidden) The ID of the scalability group.

Activation Status	(Hidden) Check the device status in a cluster. If the device boots successfully, the Active status displays. If the device fails to activate, the Activation Failed status displays.
--------------------------	--

Manage How Groups for Network Functions are Displayed

Use the buttons at the top of the **Managed Devices** pane to affect the display of hierarchical groups, NFs and their associated devices.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, you can use the following buttons to manage how devices are displayed:

Refresh	Click to refresh the data displayed on the screen for hierarchical groups, NFs and their associated devices.
Collapse All	Click to collapse all folders.

View Serial Numbers for a Physical Device

Primary and secondary serial numbers of managed physical devices can be displayed by enabling hidden columns in the **Managed Devices** table.

Note:

Serial number information is pulled from a physical device through SNMP. Virtual devices return a value of N/A.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click on the right side of a column header.
The arrow icon appears with a drop-down menu.
3. Mouse over the **Columns** selection and click and the column options that you want to enable:
 - **Primary Serial Num**—Enables the Primary Serial Number column in the **Managed Devices** table.
 - **Secondary Serial Num**—Enables the Secondary Serial Number column in the **Managed Devices** table.

Export Device Information from Device Manager

You can export network function (NF) device information to your local system (PC, server, and so on) in the format of a comma-separated values (CSV) file which allows data to be saved in a table-structured format for auditing or management purposes.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the NF and click **Save to file**.
3. In the dialog box that appears, click **OK** to download the information in the form of a CSV file to your system.

 **Note:**

The information in the CSV file that is saved to your system corresponds to the NF information displayed in the **Managed Devices** pane.

Export Detailed Device Information from Device Manager

You can also export detailed network function (NF) device information from the **Device details** pane in Device Manager to your local system.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the NF and click **Show details**.
3. In the **Device Details** pane, select only the tabs for which you want to save information and click **Save to File**.

 **Note:**

Only the tabs you select are saved. For example, if you select the **Hardware** tab and next the **Software** tab, the information for these tabs is saved only.

4. In the dialog box that appears, click **OK** to download the information in the form of a CSV file to your system.

3

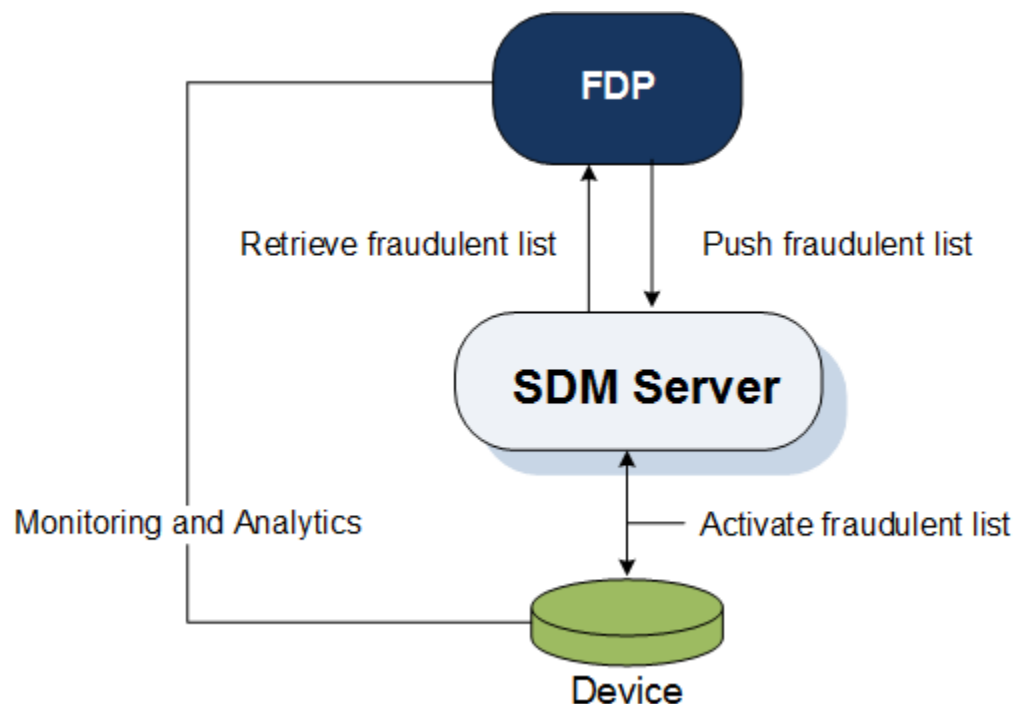
Fraud Protection Manager

Fraud Protection Manager is used to protect against fraudulent calls by using lists of phone numbers to block, allow, redirect, and limit the rate of calls. Rules are configured in Fraud Protection Manager to handle fraudulent traffic and activate fraudulent phone lists by sending a single request to activate them on multiple southbound devices.

You can use Fraud Protection Manager with the Fraud Detection and Prevention (FDP) device, or use Fraud Protection Manager manually to detect and prevent telephony fraud on southbound devices. If you want to use an FDP device, you must install the Enterprise Utilities plug-in and add the FDP device in Device Manager. See the [Device Manager](#) chapter for more information about adding a device.

The Fraud Protection Manager feature can be automated by registering Oracle Communications Session Delivery Manager (SDM) with a fraud detection device. SDM acts as a fraud update receiver that receives fraud updates from the FDP device and relays these updates to southbound devices, such as an ESBC to automatically stop fraudulent activity in the network. The FDP device can support multiple southbound devices to create a list of blacklist, white list, rate limit, and redirect information by monitoring calls, which is based on the data present in the network. SDM maintains a global fraudulent list which can originate from fraud detection devices, which in turn is shared with southbound devices for them to take further actions.

Figure 3-1 Fraud Protection Manager with an FDP device



When you use the Fraud Protection Manager feature manually, you can import and manage fraudulent lists in SDM, which then shares these lists with devices to take further actions.

Fraud Protection Manager Search Filters

The following filters can be used in Fraud Protection Manager when you use the **Search** function. Refer to individual search sections in this chapter for more information about the different search criteria that you can use for different Fraud Protection Manager search operations.

- Standard wild card * and ? characters are supported.
 - * matches 0 or more characters.
 - ? matches 1 character.
- Search filters containing wild card characters can be partial words that are case-sensitive. The following searches for the word "Boston" as it would appear in the database are correct:
 - **Bost***
 - **Bos???**
 - **Bos?on**

The following example shows an incorrect search for the word "Boston", because the search word does not follow the case-sensitive rule for the way that word would appear in the database:

- **bost***
- Search filters containing no wild card characters and that are case-sensitive result in an exact match.

Configure a Fraud Detection and Prevention Device Registration

You can register Oracle Communications Session Delivery Manager (SDM) with a Fraud Detection and Prevention (FDP) device, so that the FDP device can send automatic Fraud Protection List (FPL) updates to SDM. You can later schedule these updates to be sent from SDM to southbound devices. The updates are then activated on these devices.

Add a Fraud Detection and Prevention Device Registration

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud Detection devices** pane, click **Add**.
3. In the **Add registration** dialog box, complete the following fields:

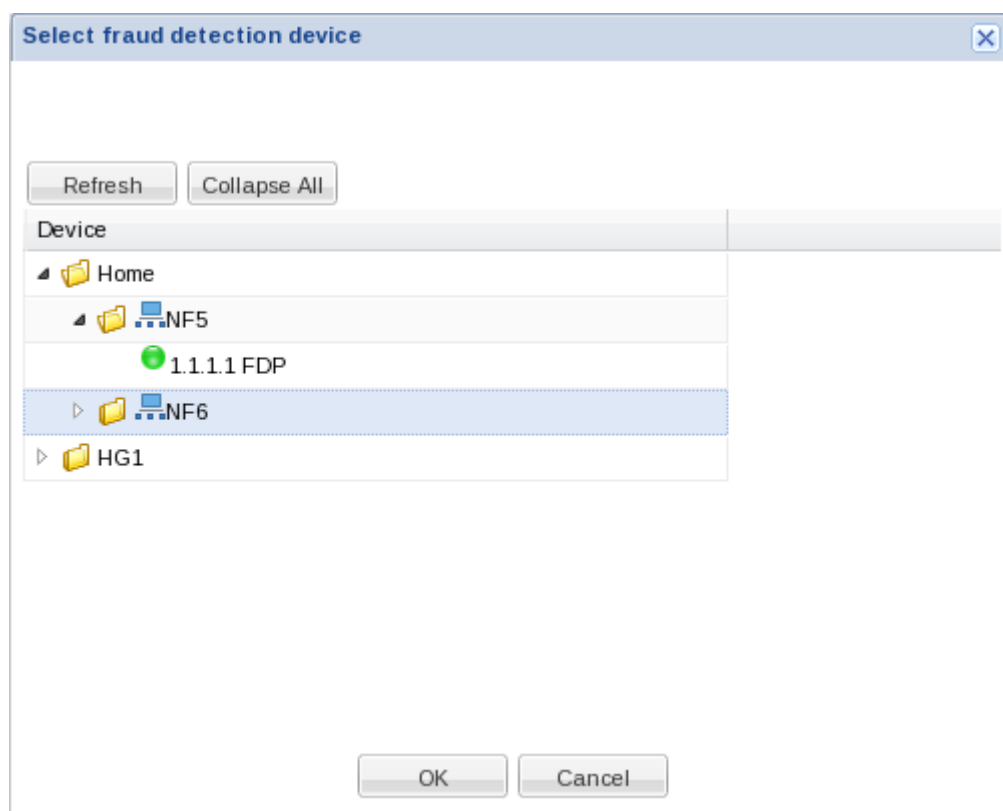
Registration name	The registration name for the FDP device. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
--------------------------	---

Fraud detection device	<p>The FDP device that you want to register. Click the ellipsis button (...) to select In the Select fraud detection device dialog box, navigate the folder group hierarchy and select the FDP device from the network function (NF) and click OK.</p> <p>You must add the folder structure, install the Enterprise Utilities plugin, and specify the FDP network function (NF) type in Device Manager before you can select a FDP device.</p>
Description field	The description of the FPD registration.
Username field	<p>The user name of the SDM user account that the selected FDP device uses to authenticate with SDM when pushing fraud update notifications. Note that the user must have full Fraud protection list privileges. Use the following steps to set these privileges:</p> <ol style="list-style-type: none"> a. Go to Security Manager, User management, Groups, and click the Applications tab. b. Expand the Application folder. c. Select Fraud protection list and set the privileges to Full.
Password field	This password of the SDM user account that the selected FDP device uses to authenticate with SDM when pushing fraud update notifications.

 **Note:**

When registering an FDP, you must always configure an expiration time for the SDM user added in the **Add registration** dialog box. For non-Admin users the default value is 15 minutes and for Admin users there is no default setting. If you use an Admin user without an expiration time set, the registration will fail. Oracle recommends using a non-Admin user when registering an FDP.

The following figure provides an example shows the FDP device (1.1.1.1 FDP) in the **Select fraud detection device** dialog box:



4. In the **Add registration** dialog box, click **OK**.

The FDP device is registered with the SDM, and can begin sending telephony fraud updates to SDM.

Register a Fraud Detection and Prevention Device

Register Oracle Communications Session Delivery Manager (SDM) with a Fraud Detection and Prevention (FDP) Device that you added. This action provides the FDP device with the information necessary for it to communicate with OCSDM.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** page, select an FDP from the **FDP** table and click **Register**.

Re-register a Fraud Detection and Prevention Device

Use this task if you need to re-register a Fraud Detection and Prevention (FDP) device in Oracle Communications Session Delivery Manager (OCSDM).

For example, you need to re-register an FDP device after performing backup and restore operations for an OCSDM cluster, or when adding a new member node to an OCSDM cluster.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** page, select an FDP from the **FDP** table and click **Unregister**.
3. Reselect the FDP and click **Register**.

Edit a Fraud Detection and Prevention Device Registration

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** pane, click **Edit**.
3. In the **Edit registration** dialog box, edit any of the following fields:

Registration name	(Read-only) The registration name for the FDP device.
Fraud detection device	(Read-only) The registered FDP device.
Description field	The description of the FDP registration.
Username field	The user name of the SDM user account that the selected FDP device uses to authenticate with SDM when pushing fraud update notifications.
Password field	This password of the SDM user account that the selected FDP device uses to authenticate with SDM when pushing fraud update notifications.

 **Note:**

When registering an FDP, you must always configure an expiration time for the SDM user added in the **Edit registration** dialog box. For non-Admin users the default value is 15 minutes and for Admin users there is no default setting. If you use an Admin user without an expiration time set, the registration will fail. Oracle recommends using a non-Admin user when registering an FDP.

4. Click **OK**.

View Fraud Detection and Prevention Device Registration Information

The **Fraud Detection devices** pane has a list of Fraud Detection and Prevention (FDP) devices that Oracle Communications Session Delivery Manager (SDM) has registered with to receive fraud updates.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** pane, you can view the following FDP device registration column information:

Registration name	The unique, specified registration name for the FDP device.
Name	The FDP device group name. This is the parent group name of the FDP device(s) that was specified when the FDP network function (NF) was added in Device Manager.
IP Address	The IP Address of the registered fraud detection device (FDP)

Status	<p>The current FDP device group status for providing fraud updates to SDM. Once the FDP device group is registered with SDM, SDM periodically checks the status of the FDP device group. The following states can occur:</p> <ul style="list-style-type: none"> • Active—The device group is registered with SDM properly, and is able to push periodic fraud updates to all cluster members. • Down—The SDM server is unable to connect or login to the FDP device group. • Impaired—The registration is partially functional. For example, the FDP device group is able to communicate with one, but not all SDM cluster members. An FDP device group treats each SDM cluster member as a separate push receiver. • Error—The FDP device group is reachable, but it cannot push incremental updates to SDM because of an error.
Status details	A description of the status, which is provided to communicate specific errors or issues that require attention.
Last event update time	The time at which the FDP device group status changed.
Description	(Hidden) The user-specified registration description of the FDP device group.

3. In the **Fraud Detection devices** pane you can also choose from the following actions to display registration information:
 - Click **Refresh** to refresh the contents of the **Fraud Detection devices** registration table.
 - Click **Show All** to display the entire registration list.

Search Fraud Detection and Prevention Device Registrations

Refer to the [Fraud Protection Manager Search Filters](#) section for more information on filtering when you use a search criteria.

1. Expand the **Fraud Protection Manager** slider and click **Administration** in the navigation pane.
2. In the **Fraud detection devices** pane, click **Search**.
3. In the **Search criteria** dialog box, complete any of the following fields to create a search criteria:

Registration name	The registration name for the FDP device. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Fraud detection device field	The FDP device name.
IP address field	The IP address of the FDP device.

Status drop-down list	Search using any of the following registered FDP device states: <ul style="list-style-type: none">• Not Registered• Ready• Full Update In Process• Update Requested• Update In Process• Not Synchronized
------------------------------	---

4. Click **OK**.

Re-synchronize Session Delivery Manager with Fraud Protection List Data

You can re-synchronize Oracle Communications Session Delivery Manager (SDM) so that SDM has all of the Fraud Protection List (FPL) data that is available.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** page, select a registered FDP from the **FDP** table and click **Re-synch**.

The FDP device sends again all updates to SDM, including any missed FPL updates that occurred since updates were last received by SDM.

Unregister a Fraud Detection and Prevention Device

Unregister a Fraud Detection and Prevention (FDP) Device with Oracle Communications Session Delivery Manager (SDM) so that it does not receive automatic fraud updates.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** page, select a registered FDP device from the **FDP** table and click **Unregister** to unregister the FDP device.
3. In the confirmation dialog box, click **Yes** to unregister the FDP registration so that this device no longer receives automatic fraud updates through SDM.

Register a Fraud Detection and Prevention Device

Register an unregistered Fraud Detection and Prevention (FDP) Device with Oracle Communications Session Delivery Manager (SDM) so that it can receive automatic fraud updates.

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** page, select an unregistered FDP from the **FDP** table and click **Register** to register the FDP device with SDM again.
3. In the confirmation dialog box, click **Yes** to unregister the FDP registration so that this device no longer receives automatic fraud updates through SDM.

Delete a Fraud Detection and Prevention Device Registration

1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud detection devices** pane, select a registered fraud detection device from the table, and click **Delete**.
3. Click **OK**.

The Fraud Detection and Prevention (FDP) device registration is deleted from Oracle Communications Session Delivery Manager (SDM).

About Fraud Protection Lists

A Fraud Protection List (FPL) is a global, user-specified list with a unique name that contains list type entries (Black list, White list, Rate limit, and Call redirect) that you can specify data type and data type format parameters. An FPL can also contain data entered manually or data generated by a device. An FPL is used by Oracle Communications Session Delivery Manager (SDM) to push targeted fraud updates from a Fraud Detection and Prevention device to southbound devices that are capable of detecting telephony fraud, such as an ESBC.

Fraud Protection List Type Entries

The following table shows the FPL list type entries you can manage for the ingress realm of a southbound device:

Black list	Use this FPL entry to specify a fraudulent call based on the destination phone number or URI. You can add a known fraudulent destination to the blacklist by prefix or by fixed number. When a device receives a call to an entry on the blacklist, the system rejects the call according to the specified SIP response code.
White list	Use this FPL entry to manage any exception to the blacklist, such as if a prefix such as 49 555 123 is blocked by the blacklist. This also blocks calls to individual numbers starting with this prefix, such as 49 555 123 666. If you add a prefix or individual number to the white list, the system allows calls to the specified prefix and number. Continuing with the previous example, if you add 49 555 123 6 to the white list, the system allows calls to 49 555 123 666, which was blocked by the blacklist entry of 49 555 123.
Rate limit	Use this FPL entry to limit the loss of money, performance, and availability that an attack might cause. While local ordinances may not allow you to completely block or suppress communication, as with a blacklist, you may want to reduce the impact with rate limiting until a network engineer can analyze an attack and plan remediation. Note that rate limiting may not function immediately after a High Availability switch over because the newly active system must re-calculate the call rate before it can apply rate limiting.
Call redirect	Use this FPL entry to send a fraudulent call to an Interactive Voice Response (IVR) system, or to a different route. For example, you can intercept and redirect a call to a revenue-share fraud target in a foreign country to an end point that defeats the fraud. For example, you can redirect subscribers dialing a particular number and URI to an announcement to make them aware that an account is compromised and what they should do. You can use an external server to provide such an announcement or you can use the E-SBC media playback function.

Fraud Protection List Data Types

The following data type of the Session Initiation Protocol (SIP) to or from header that is used in an FPL black list, white list, rate limit or call direct entry:

from-hostname	The hostname from the SIP FROM header.
from-phone-number	The phone number from the SIP FROM header.
from-username	The user name from the SIP FROM header.
to-hostname	The hostname from the SIP TO header.
to-phone-number	The phone number from the SIP TO header.
to-username	The user name from the SIP TO header.
user-agent-header	The SIP User-Agent header. This header contains information about the client user agent originating the request.

Fraud Protection List Data Type Formats

The following table describes the required formats for each data type Session Initiation Protocol (SIP) to or from header that is used in an FPL black list, white list, rate limit or call direct entry:

hostname	The exact IP address or Fully Qualified Domain Name (FQDN).
username	The exact user name. For example: joe.user or joe_user.
user-agent-header	The exact text match to the SIP User-Agent header. For example: equipment vendor information.
phone-number	<p>The following characters are allowed for a phone number:</p> <ul style="list-style-type: none"> Use the asterisk (*) character to indicate prefix matching, but only at the end of the pattern. For example, use 555* not *555. Do not use the asterisk character in any other patterns, for example, in brackets [], parentheses (), or with an x. Use the bracket [] characters to enclose ranges in a pattern. Syntax: [min-max]. For example: 555[0000-9999]. Use parentheses () to enclose optional digits in a pattern. For example: 555xx(xxxx) means 555 with between 2 and 4 following digits. Use the character x as a wildcard at the end of a dial pattern to mean 0-9. For example: 555xxx means a number starting with 555 followed by 3 digits. <p>No leading zeroes or plus (+) characters are allowed.</p>

Configure Fraud Protection Lists

Fraud Protection Lists (FPLs) are used and created to protect individuals from fraudulent calls.

You can add, edit, import, upload and copy an FPL, manage FPL list entries, and assign and re-synchronize an FPL with a Fraud Detection and Prevention (FDP) device. You can also schedule a specific time to push an FPL to an associated southbound device.

Add a Fraud Protection List

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, click **Add**.
3. In the **Add FPL** dialog box, complete the following fields:

Name	The unique FPL name that is used by SDM to identify the FPL. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Description	The FPL description.
Device file name	The FPL file name that exists on the southbound device.
Realm originated from	The realm instance choices that come from this device for an individual FPL entry. Click the ellipses (...) button. In the Select managed device dialog box, navigate the folder hierarchy and network function (NF) and select the southbound device from which the ingress realm originates.

4. Click **OK**.

The FPL is added to the SDM database.

Add a Fraud Protection List Entry

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL to which you want to make changes from the **FPL** table and click **Manage**.
3. In the **Edit FPL entries** pane, select from any of the following FPL type entry tabs that you want to add an FPL entry and click **Add**.

Refer to the [Fraud Protection List Type Entries](#) section for more information about the following FPL types:

- **Black list**
- **White list**
- **Rate limit**
- **Call redirect**

4. Depending on the FPL type, the following fields can appear in the dialog box used to add lists:

Data type drop-down list	Black and white lists, and Rate limit FPL types use the data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about data type parameters.
---------------------------------	---

Match value field	Black and white lists, and Rate limit FPL types use the exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type Formats section for more information on the formats required for this parameter.
Realm drop-down list	Black and white lists, and Rate limit FPL types use the name of the SIP realm that is configured on the device. The SIP realm is associated with the match value.
Calls per second field	Rate limit FPL types only use the number of call attempts per second.
Max active calls field	Rate limit FPL types only use the maximum number of simultaneous active calls.

5. Click **OK**.

Import a Fraud Protection List

You can create a new Fraud Protection List (FPL) file by importing the contents of an existing template configuration FPL file from a local file that has an .xml, .gz, or .gzip format.

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, click **Import**.
3. In the **Import FPL file** dialog box, complete the following fields:

Name field	The unique FPL name that is used by SDM to identify the FPL. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Description field	The FPL description.
Device file name field	The FPL file name that exists on the southbound device.
Realm originated from field	The realm instance choices that come from this device for an individual FPL entry. Click the ellipses (...) button. In the Select managed device dialog box, navigate the folder hierarchy and network function (NF) and select the southbound device from which the realm originates and click OK .
File field	Click Browse . In the File Upload dialog box, navigate to and select the file on your system that you want to upload and click Open .

4. Click **OK**.

The contents of the selected file are copied to the new FPL.

Upload a Fraud Protection List from a Device

You can create a new Fraud Protection List (FPL) file by importing an FPL file from an existing device.

Pre-requisites: Before you choose a device as the realm source, you must first add and load this device in Configuration Manager. Refer to the [Associate Devices with Session Element Manager](#) section for more information.

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, click **Upload**.
3. In the **Upload FPL file** dialog box, complete the following fields:

Name field	The unique FPL name that is used by SDM to identify the FPL. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Description field	The FPL description.
Device file name field	The FPL file name that exists on the southbound device.
Selected device field	Click the ellipses (...) button. In the Select managed device dialog box, navigate the folder hierarchy and network function (NF) and select the southbound device from which the realm originates.
File from selected device drop-down list	Select from the list of FPL files that are populated from the device selected in the previous field.

4. Click **OK**.

The contents of the selected device file are copied to the new FPL.

Copy Fraud Protection List Contents to Another Fraud Protection List

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select an FPL and click **Copy**.
3. In the **Copy FPL** dialog box, select from the following options:

- **Copy all entries** (Default)
- **Copy user-modified entries only**

4. In the second **Copy FPL** dialog box that appears, complete the following options:

Source FPL field	(Read-only) The FPL name that you selected from the FPL management tab.
Destination FPL field	The unique FPL destination name. There must be no space before, within, or after the name you enter. The first character

	must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Description box	The FPL description.
Device file name field	The FPL file name that exists on the southbound device.
Realm originated from field	The realm instance choices that come from this device for an individual FPL entry. Click the ellipses (...) button. In the Select managed device dialog box, navigate the folder hierarchy and network function (NF) and select the southbound device from which the ingress realm originates.

5. Click **OK**.

The contents of the selected FPL are copied to the new FPL.

Assign Fraud Detection and Prevention Device to a Fraud Protection List

You can assign a single registered Fraud Detection and Prevention (FDP) device to one or multiple Fraud Protection Lists (FPLs).

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select an FPL from the **FPL** table and click **Assign**.
3. In the **Assign FPL** dialog box, complete the following fields.

Name field	The name of the selected FPL.
Assigned to drop-down list	Select from the available FDP device(s) that are registered with Oracle Communications Session Delivery Manager (SDM). An FDP device is added to Oracle Communications Session Element Manager through the Enterprise Utilities product plug-in when you select FDP as the Network Function (NF) type.

4. Click **OK**.

When the FDP device pushes FPL updates to SDM, SDM uses the assigned FPL to reconcile the FPL updates.

Unassign Fraud Detection and Prevention Device to a Fraud Protection List

You can unassign a single registered Fraud Detection and Prevention (FDP) device from one or multiple Fraud Protection Lists (FPLs).

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select an FPL from the **FPL** table and click **Un-assign**.
3. In the confirmation dialog box, click **Yes**.
4. In the **Success** dialog box, click **OK**.

Manage Fraud Protection Lists

Edit a Fraud Protection List

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select an existing FPL from the **FPL** table and click **Edit**.
3. In the **Edit FPL** dialog box, modify the following applicable fields:

Name	(Read-only) The unique FPL name that is used by SDM to identify the FPL. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore (_) are supported. A space cannot precede or trail the name.
Description	The FPL description.
Device file name	The FPL file name that exists on the southbound device.
Realm originated from	This field cannot be edited unless the referenced device is no longer available. If the device is no longer available, click the ellipses (...) button. In the Select managed device dialog box, navigate the folder hierarchy to the southbound device from which the realm originates.

4. Click **OK**.

Manage a Fraud Protection List Entry

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL to which you want to make changes from the **FPL** table and click **Manage**.
3. In the **Modify FPL** pane, select from the following FPL entry tabs, and click **Add** to add an entry:
 - **Black list**
 - **White list**
 - **Rate limit**
 - **Call redirect**
4. In the dialog box for the above FPL entry, the following parameters are retrieved dynamically from the ingress realm of the southbound device associated with the FPL:

Data Type	The data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about valid data type parameters.
Match value	The exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type

	Formats section for more information on the formats required for this parameter.
Ingress realm	Select to change the ingress realm instance, which is specified on the southbound device, from the drop-down list. Realm instances are obtained from the southbound device. The southbound device uses this parameter to route traffic. Refer to your device documentation for more information about ingress realms.
Calls per second	(Rate limit only) The number of call attempts per second from 0 to 65535. Enter zero for unlimited call attempts.
Max active calls	(Rate limit only) The maximum number of simultaneous active calls from 0 to 65535. Enter zero for unlimited active calls.
Redirect target	(Call redirect only) The SIP redirect server which can be identified by using any one of the following values: session agent, session agent group name, hostname, or IP address.

5. Click **OK** to finish adding the entry to the FPL entry.

The entry appears in the FPL entry tab.

Edit a Fraud Protection List Entry

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL to which you want to make changes from the **FPL** table and click **Manage**.
3. In the **Edit FPL entries** pane, select from the following FPL entry tabs, select an entry, and click **Edit**.

Refer to the [Fraud Protection List Type Entries](#) section for more information about the following FPL types:

- **Black list**
- **White list**
- **Rate limit**
- **Call redirect**

4. In the edit list dialog box, edit the following fields.

Data type drop-down list	The data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about data type parameters.
Match value field	The exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type Formats section for more information on the formats required for this parameter.
Realm drop-down list	You must first click the drop down-list arrow first to select the name of the SIP realm that is configured on the device. The SIP realm is associated with the match value. If the realm for which you are looking does not appear in the drop-down list, you can then type this realm name in the field.

Calls per second field	(Rate limit only) The number of call attempts per second from 0 to 65535. Enter zero for unlimited call attempts.
Max active calls field	(Rate limit only) The maximum number of simultaneous active calls from 0 to 65535. Enter zero for unlimited active calls.
Redirect target field	(Call redirect only) The SIP redirect server which can be identified by using any one of the following values: session agent, session agent group name, hostname, or IP address.

- Click **OK**.

Copy a Fraud Protection List Entry

You can copy values from one Fraud Protection List (FPL) entry to build a new entry.

- Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
- In the **FPL management** tab, select the FPL to which you want to make changes from the **FPL** table and click **Manage**.
- In the **Modify FPL** pane, choose from the following FPL entry tabs, select an entry, and click **Copy**:
 - Black list**
 - White list**
 - Rate limit**
 - Call redirect**
- In the copy list dialog box, edit any of the following fields that you are copying.

Data type drop-down list	The data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about data type parameters.
Match value field	The exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type Formats section for more information on the formats required for this parameter.
Realm drop-down list	The name of the SIP realm that is configured on the device. The SIP realm is associated with the match value.
Calls per second field	(Rate limit only) The number of call attempts per second from 0 to 65535. Enter zero for unlimited call attempts.
Max active calls field	(Rate limit only) The maximum number of simultaneous active calls from 0 to 65535. Enter zero for unlimited active calls.
Redirect target field	(Call redirect only) The SIP redirect server which can be identified by using any one of the following values: session agent, session agent group name, hostname, or IP address.

- Click **OK**.

The copied entry appears as a new entry in the FPL entry tab.

View Fraud Protection List Entry Information

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL for which you want to view entries from the **FPL** table and click **Manage**.
3. In the **Modify FPL** pane, you can view the following table columns for each FPL **Black list**, **White list**, **Rate limit**, and **Call redirect** entry tab:

Data type	The data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about data type parameters.
Match value	The exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type Formats section for more information on the formats required for this parameter.
Realm	The name of the SIP realm that is configured on the device. The SIP realm is associated with the match value.
Calls per second field	(Rate limit only) The number of call attempts per second from 0 to 65535. Enter zero for unlimited call attempts.
Max active calls field	(Rate limit only) The maximum number of simultaneous active calls from 0 to 65535. Enter zero for unlimited active calls.
Redirect target field	(Call redirect only) The SIP redirect server which can be identified by using any one of the following values: session agent, session agent group name, hostname, or IP address.

4. (Optional) Click **Refresh** to refresh the **Fraudulent list** table contents in each FPL **Black list**, **White list**, **Rate limit**, and **Call redirect** entry tab.

Search Fraud Protection List Entry Information

Refer to the [Fraud Protection Manager Search Filters](#) section for more information on filtering when you use a search criteria.

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL for which you want to view entries from the **FPL** table and click **Manage**.
3. In the **Modify FPL** pane, select **Search** in the **Black list**, **White list**, **Rate limit**, or **Call redirect** entry tab.
4. (Optional) In the **Fraudulent list** table, click **Search** to search the contents in each FPL **Black list**, **White list**, **Rate limit**, and **Call redirect** entry tab.
5. In the **Search criteria** dialog box, complete the following fields.

Data type drop-down list	The data type of the Session Initiation Protocol (SIP) to or from header, or SIP user-agent header. See the Fraud Protection List Data Types section for more information about data type parameters.
Match value field	The exact match value that corresponds to the data type. For example, the match value could be a type of data such as a phone number prefix, source or destination IP address. See the Fraud Protection List Data Type Formats section for more information on the formats required for this parameter.
Realm field	The name of the SIP realm that is configured on the device. The SIP realm is associated with the match value.
Calls per second field	(Rate limit only) The number of call attempts per second from 0 to 65535. Enter zero for unlimited call attempts.
Max active calls field	(Rate limit only) The maximum number of simultaneous active calls from 0 to 65535. Enter zero for unlimited active calls.
Redirect target field	(Call redirect only) The SIP redirect server which can be identified by using any one of the following values: session agent, session agent group name, hostname, or IP address.

6. Click **OK**.

Delete a Fraud Protection List Entry

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL to which you want to make changes from the **FPL** table and click **Manage**.
3. In the **Modify FPL** pane, choose from the following FPL entry tabs, select an entry, and click **Delete**:
 - **Black list**
 - **White list**
 - **Rate limit**
 - **Call redirect**
4. In the confirmation dialog box, click **Yes**.

The entry no longer appears in the FPL entry tab.

Unassign a Fraud Detection and Prevention Device from a Fraud Protection List

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select an FPL from the **FPL** table and click **Un-assign**.
3. In the confirmation dialog box, click **OK**.

Any FPL updates from the Fraud Detection and Prevention (FDP) are no longer reconciled by the Oracle Communications Session Delivery Manager (SDM).

View Fraud Protection List Information

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, you can view the following Fraud Protection List (FPL) column information:

Name	The unique FPL name.
Description	(Hidden) The user-specified description of the FPL.
Device file name	(Hidden) The name of the xml file which is defined and used by SDM when the FPL is pushed to the device.
Ingress realm originated from	(Hidden) The southbound device target name whose realm configuration instances are the choices for the ingress realm of any entry in a blacklist, white list, rate limit, and call redirect.
Creation date	The last date and time that the FPL was added.
Modified date	The last date and time that the FPL was modified.
Status	The FPL status, which is either in the <i>Updated successfully</i> or <i>Failed reconciliation</i> state.
Assigned	The name of the registered fraud detection device (FDP) that is assigned to the FPL.

3. (Optional) Click **Refresh** to refresh the **FPL management** tab table contents.
4. (Optional) Click **Search** to search the **FPL management** tab table contents. In the **Search criteria** dialog box, you can search using the criteria:

Name	The FPL name.
Device file name	The FPL file name of the southbound device.
Creation date field	Click the calendar icon to select the date and time for when the FPL was created.
Modified date field	Click the calendar icon to select the date and time for when the FPL was modified.
Status drop-down list	Select the status of the FPL on which you are searching: Success , Updated successfully , or Failed reconciliation .
Assigned	The name of the registered fraud detection device (FDP) that is assigned to the FPL.

Search for a Fraud Protection List

Refer to the [Fraud Protection Manager Search Filters](#) section for more information on filtering when you use a search criteria.

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, click **Search**.

3. In the **Search criteria** dialog box, complete any of the following fields to create a search criteria:

Name field	The unique FPL name that is used by SDM to identify the FPL. There must be no space before, within, or after the name you enter. The first character must be alphabetic. A dash (-) and an underscore () are supported. A space cannot precede or trail the name.
Device File name field	The FPL file name.
Creation date field	Click the calendar icon to select the date and time for when the FPL was created.
Modified date field	Click the calendar icon to select the date and time for when the FPL was modified.
Status field	Select from the following FPL status search options: <ul style="list-style-type: none"> • Success • Updated successfully • Failed reconciliation • In Progress • Copy in Progress • FDP Update in Progress • FDP Update Failed • Export in Progress • Export Failed • Import in Progress • Import Failed • Upload in Progress • Upload Failed • Failed
Assigned field	The name of the registered fraud detection device (FDP) that is assigned to the FPL.

4. Click **OK**.

Delete a Fraud Protection List

1. Expand the **Fraud Protection Manager** slider, and click **Fraud protection list**.
2. In the **FPL management** tab, select the FPL and click **Delete**.
3. In the confirmation dialog box, click **OK**.



Note:

An FPL cannot be deleted if it is currently associated with a Fraud Detection and Prevention (FDP) device or with a push task.

The FPL is deleted from the SDM database.

Configure Fraud Protection List Push Task Updates

You can add new Fraud Protection List (FPL) update tasks that are on-demand, scheduled, or automatic, and schedule a specific time to push them to associated southbound devices on which they are executed.

After an FPL push task is executed, it must be committed to unlock the targeted devices that are associated with the FPL push task. Only FPL push tasks with a status of **Success**, **Failed**, **Aborted**, **AbortFailed**, or **CommitFailed** can be committed. When an FPL push task is committed automatically or manually, all targeted devices associated with this FPL push task are unlocked and this FPL push task can no longer be modified or rolled back. You must create a new FPL push task to implement new changes.

Add a Fraud Protection List Push Task

You can schedule a specific time to push a Fraud Protection List (FPL) to its associated southbound devices by adding a push task.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab.
3. Below the **FPL push tasks** table, click **Add**.
4. In the **Add FPL push task configuration** pane, complete the following fields:

Name field	The unique, user-specified name assigned to the push task that is an alpha-numeric value from 1 to 24 characters in length with no spaces.
Task type drop-down list	<p>Select from the following push task types:</p> <ul style="list-style-type: none"> • On demand— Start the task anytime. • Schedule— Plan a specific time to start the task. • Auto FDP—No user intervention required. FPL updates are pushed regularly to Oracle Communications Session Delivery Manager (SDM) from the Fraud Detection and Prevention (FDP) device. SDM reconciles these updates with the specified FPL and pushes the result after reconciliation to the device(s). If the reconciliation fails, then an error is logged. If the pass through status of the FPL push task is NotScheduled or Committed then the pass through push task is allowed to start immediately (the Start now status). If the pass through push task is running and FPL updates are sent to SDM at the same time, then SDM queues the FPL updates and waits until the push task is finished, at which time SDM reconciles with the queued FPL updates.

FPL drop-down list	Select the Fraud Protection List (FPL) name that is applied to the device(s).
Start date and time field	This option is available only if the Task type is Schedule . Select a start date for the push task is scheduled to start by clicking the calendar icon and specify time entries in the Time fields by selecting the hour, minute and second respectively by typing the numbers in the text box or using the arrows.
auto Commit checkbox	You can use this option if the Task type is On demand or Schedule only. If the Task type is set to Auto FDP , the auto commit function is on automatically and cannot be modified. When a push task completes, but is not committed, it retains a lock on all its targeted devices so that no other operations can be performed on them until the push task is successfully committed and its devices are unlocked. Check the check box to automatically commit the push task after the successful execution of the push task. If the check box is unchecked, you have to manually commit the push task. Refer to the Commit a Fraud Protection List Push Task Manually section for more information.

5. Below the **Device group tasks** table, click **Manage**.
6. In the **Select Device** dialog box, expand a device folder in the **Managed devices** table, select a device row, and click **Add**.

The device, its network function and folder structure moves to the **Targeted Devices** table and the folder structure is collapsed.

Note:

A work order has the following limitations:

- The device must be capable of using the telephony fraud feature.
- A push task is limited to one platform and software version at a time.
- In the case of an HA device pair, the FPL push task is applied to both devices.
- All devices must have the same platform, software version, and same redundancy type (HA or standalone).

Note:

If you receive a **Warning** message that says the FPL file on the device you adding does not match the FPL that you are using for the push task, you must use Configuration Manager or the device ACLI to change the FPL file name on the device to match the FPL of your FPL push task in order for the FPL push task to be used with the device you are adding. Refer to the device documentation for more information about changing the FPL file name on the device.

7. Repeat the previous steps to add additional targeted devices. Up to twenty devices can be added to a push task.



Note:

Device filtering is applied after the first device is selected.

8. Click **OK**. The device(s) appear in the **Device group tasks** table, which displays the network function (NF) name and its device(s).
9. Click **Apply**.
10. In the success dialog box, click **OK**.

The FPL push task that you specified appears in the **FPL push tasks** table.

Manage Fraud Protection Push Task Updates

Edit a Fraud Protection List Push Task



Note:

A push task can only be modified if its status is either **PartiallyConfigured** or **NotScheduled**.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab, select the Fraud Protection List (FPL) that you want to modify and click **Edit**.



Note:

If the push task cannot be edited because it is configured or you not have permission to modify it, this **Edit** button changes to **View** and the **Edit FPL push task configuration** pane is in read-only mode.

3. In the **Edit FPL push task configuration** pane, you can modify the following fields:

Name field	(Read-only) The unique, user-specified name assigned to the push task that is an alpha-numeric value from 1 to 24 characters in length with no spaces.
Task typedrop-down list field	<p>Select from the following push task types:</p> <ul style="list-style-type: none"> • On demand— Start the task anytime. • Schedule— Plan a specific time to start the task. • Auto FDP—No user intervention required. FPL updates are pushed regularly to Oracle Communications Session Delivery Manager (SDM) from the Fraud Detection and Prevention (FDP) device. SDM reconciles these updates with the specified FPL and pushes the result after reconciliation to the device(s). If the reconciliation fails,

	then an error is logged. If the pass through status of the FPL push task is NotScheduled or Committed then the pass through push task is allowed to start immediately (the Start now status).
FPL drop-down list	Select the Fraud Protection List (FPL) name that is applied to the device(s).
Start date and time field	This option is available only if the Task type is Schedule . Select a start date for the push task is scheduled to start by clicking the calendar icon and specify time entries in the Time fields by selecting the hour, minute and second respectively by typing the numbers in the text box or using the arrows.
Auto commit checkbox	You can use this option if the Task type is On demand or Schedule only. If the Task type is set to Auto FDP , the auto commit function is on automatically and cannot be modified. When a push task completes, but is not committed, it retains a lock on all its targeted devices so that no other operations can be performed on them until the push task is successfully committed and its devices are unlocked. Check the check box to automatically commit the push task after the successful execution of the push task. If the check box is unchecked, you have to manually commit the push task. Refer to the Commit a Fraud Protection List Push Task Manually section for more information.

- In the **Device group tasks** table and select the Network Function (NF) and click **Manage** to edit device in the push task.
- In the **Select Device** dialog box, expand a device folder in the **Managed devices** table, select a device row, and click **Add** to add an additional device or if you want to remove a device from the push task, select the device row and click **Remove**.

The device, its network function and folder structure moves to the **Targeted devices** table and the folder structure is collapsed.

- The device must be capable of using the fraud protection feature.
- A push task is limited to one platform and software version at a time.
- In the case of an HA device pair, the FPL push task is applied to both devices.

 **Note:**

If you receive a **Warning** message that says the FPL file on the device you adding does not match the FPL that you are using for the push task, you must use Configuration Manager or the device ACLI to change the FPL file name on the device to match the FPL of your FPL push task in order for the FPL push task to be used with the device you are adding. Refer to the device documentation for more information about changing the FPL file name on the device.

- Repeat the previous steps to add or remove additional targeted devices. Up to twenty devices can be added to a push task.

 **Note:**

Device filtering is applied after the first device is selected.

7. Click **OK**. The device(s) appear in the **Device group tasks** table, which displays the network function (NF) name and its device(s).
 8. Click **Apply**.
 9. In the success dialog box, click **OK**.
- The changes that you made appear in the **FPL push tasks** table.

Commit a Fraud Protection List Push Task Manually

A Fraud Protection List (FPL) push task can be committed manually if the **Auto commit** checkbox is not checked in the **FPL push task configuration** pane.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab and select an FPL push task from the FPL push tasks table and click **Commit**.
3. In the confirmation dialog box, click **Yes**.
4. Click **Refresh** to confirm the FPL push task status changed from **Success** to **Committed**.

Update Fraud Protection List Changes Manually When Automatic Updates are Enabled

When the Fraud Protection Manager is configured to automatically push notifications to devices, any user changes made to a Fraud Prevention List (FPL) are delivered to the devices on the next incident reported by the FDP that is registered to the FPL.

For changes that need to be pushed to the device immediately, use the following procedure to manually push changes.

1. Stop the automation on the current FPL push task.
2. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
3. Click the **Device association** tab, select the Fraud Protection List (FPL) that you want to modify and click **Edit**.
4. Make the necessary changes to the FPL.
5. In the **Edit FPL push task configuration** pane, set the **Task type** drop-down list to **On demand**.
This pushes your FPL changes to the device.
6. Create a new automatic FPL push task once the manual push task completes. For details on creating an FPL push task, see "Add a Fraud Protection List Push Task".

Stop Fraud Protection List Push Task Updates

Until the FPL push task is committed, you can stop it and perform a rollback to restore the original configuration settings if the push task is in a **WaitStarting**, **Failed**, **Success** or **Scheduled** state.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab, and select the FPL push task that you want to roll back from the **FPL push tasks** table and click **Abort**.
3. In the confirmation dialog box, click **Yes**.

After an FPL push task with a **Failed** or **Success** state is aborted; all changes on all targeted devices are rolled back to their previous state before the FPL push task was executed. If the FPL push task was in a **WaitStarting** or **Scheduled** when it was aborted, the FPL push task status changes to **NotScheduled**.

Copy a Fraud Protection List Push Task

When a Fraud Protection List (FPL) push task is executed successfully, it cannot be modified, which includes adding devices. However, you can copy an existing FPL push task and save it as a new FPL push task. The new FPL push task can then be applied to a different set of devices. Copies of an FPL push task can be used to divide large numbers of devices into smaller groups of devices that repeat the same push task.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab, and select the FPL push task that you want to copy from the **FPL push tasks** table and click **Copy**.
3. In the **Copy FPL push task configuration** pane, provide a new name for the push task and make any other changes for the new FPL push task. See the [Edit a Fraud Protection List Push Task](#) section for more information about modifying these parameters or adding or removing devices.
4. Click **Apply**.
5. In the success dialog box, click **OK**.

The changes that you made appear in the **FPL push tasks** table.

Resubmit a Device Group Push Task

You can resubmit a push task to start execution for the targeted device group network function (NF) if the status of the push task is in the **Failed**, **ResetToReady**, or **RollbackFailed** state.

Note:

You must wait for the running push task to complete before you can resubmit it. A warning appears if you try to resubmit a push task that is currently running.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab to access the Fraud Protection List (FPL) push task information.
3. In the **Device group tasks** table, select the push task row and click **Resubmit**.

View Fraud Protection List Push Task Information

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.

2. Click the **Device association** tab to access the Fraud Protection List (FPL) push task information.
3. In the **FPL push tasks** table, the following column information displays all the push tasks configured in SDM:

Name	The alpha-numeric, unique, user-specified name assigned to the push task.
Device count	The number of targeted device nodes (standalone devices or HA pairs) the push task executes. An HA pair is considered one device node.
FPL	The Fraud Protection List (FPL) name that is applied to the device(s).
Status	<p>A push task can have the following status:</p> <ul style="list-style-type: none"> • PartiallyConfigured—The configuration is incomplete. This can also be the initial state of a copied push task. • NotScheduled—The push task start time is not yet configured by the user. • Scheduled—The push task start time is configured and scheduled to begin at a specified date and time. • WaitStarting—The scheduled push task is placed into a run-waiting queue by the server's scheduler and awaits the scheduled time to start running. • Running—The push task started and is currently processing. • Success—The push task execution completed successfully, but has not yet been committed. • Failed—The push task failed during execution. • StartCommitting—The push task started the process of committing the designated changes after the Committed button was pushed. • Committing—The push task is in the process of committing the designated changes. • Committed—The changes were executed successfully by this push task and are now committed. • CommitFailed—The push task failed to commit and some of the locked resources or the auto-generated files may fail to remove. • StartAborting—The push task is in the beginning process of aborting after the Abort button is pushed. • Aborting—The push task is executing the abort process. • Aborted—The push task has been successfully aborted. All changes made on all targeted devices are rolled back and the devices retain their original state prior to the work order execution. • AbortFailed—The push task failed to abort due to a failure of a device rollback process. • LockingResource—The state when the push task locks all necessary resources. • LockResourceFailed—The push task failed to lock all necessary resources. You can restart the work order in this state.

Start time	The server start date and local time for the push task.
End time	<p>The end time is the server local time when the following conditions occur for this push task:</p> <ul style="list-style-type: none"> • The work order finished successfully and paused. • A failed condition has been met and the work order stopped as a result of the failure. • The user manually stops a work order already in progress.

View Device Group Push Tasks

The Device group tasks table displays a summary of a the best-effort device tasks that are launched or scheduled to be launched in parallel for the selected push task in the Fraud Protection List (FPL) push tasks table.

Note:

Oracle Communications Session Delivery Manager (SDM) uses a prefix name plus the name of the applied FPL configuration XML file as the compressed file name that is pushed to the device to replace the FPL file on the device. The syntax of the file is as follows: `OCSDM_<globalID>_<FPLFilename>.xml.gz`, where the `globalID` is the unique global identifier that is specified during the SDM installation, and the FPL file name. For example, `OCSDM_EastCluster_FPLConfig.xml.gz`.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab to access the Fraud Protection List (FPL) push task information.
3. In the **Device group tasks** table, view the following column information:

Name	Description
Network function	The name of the network function (NF) to which the device(s) belong.
Device group	The device group name.

Name	Description
Status	<p>A device task can have the following status:</p> <ul style="list-style-type: none"> • Ready—The push task is ready to run and waiting for the SDM scheduler to initiate the push task to start on the device. • ResetToReady— When the push task restarts, all the failed tasks are reset to this state to distinguish the initial Ready state of the device task. • Starting—The intermediate state between the Ready and Running states when users submit or resubmit the device task. • Running—The push task started and is currently processing. • Success—The push task completed successfully. • Failed—The push task failed during execution and any changes are rolled back. • RolledBack— The push task is rolled back successfully. • RollBackFailed—The push task is rolled back unsuccessfully.
Start time	<p>The SDM server start date and local time at which the push task was scheduled to start or the time when a task within a push task is started. The following criteria are used:</p> <ul style="list-style-type: none"> • If the push task has not reached its scheduled start time to start all individual tasks for this push task to display the same start time. • When an individual push task starts, it replaces the scheduled start time with the time it started processing.
End time	<p>The end time is the server local time when the following conditions occur for this device task:</p> <ul style="list-style-type: none"> • The device task finished successfully and paused. • A failed condition has been met and the device task stopped as a result of the failure.



Note:

If any one of the devices fail to do FPL file updates, then the device is automatically rolled back to the original FPL file.

4. (Optional) Click **Refresh** to update the contents in the **Device group tasks** table.
5. (Optional) Select an NF from the **Device group tasks** table and click **Logs** to view logs for the targeted device group node. Logs are maintained separately for each device group in the table.

Search for a Fraud Protection List Push Task

Refer to the [Fraud Protection Manager Search Filters](#) section for more information on filtering when you use a search criteria.

1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab, click **Search**.
3. In the **FPL push task search** dialog box, complete any of the following fields:

Name field	The unique, user-specified name assigned to the push task that is an alphanumeric value from 1 to 24 characters in length with no spaces.
FPL field	The Fraud Protection List (FPL) name that is applied to the device(s).
Status field	<p>You can filter on any of the following push task status entries:</p> <ul style="list-style-type: none"> • PartiallyConfigured—The configuration is incomplete. This can also be the initial state of a copied push task. • NotScheduled—The push task start time is not yet configured by the user. • Scheduled—The push task start time is configured and scheduled to begin at a specified date and time. • WaitStarting—The scheduled push task is placed into a run-waiting queue by the server's scheduler and awaits the scheduled time to start running. • Running—The push task started and is currently processing. • Success—The push task execution completed successfully, but has not yet been committed. • Failed—The push task failed during execution. • StartCommitting—The push task started the process of committing the designated changes after the Committed button was pushed. • Committing—The push task is in the process of committing the designated changes. • Committed—The changes were executed successfully by this push task and are now committed. • CommitFailed—The push task failed to commit and some of the locked resources or the auto-generated files may fail to remove. • StartAborting—The push task is in the beginning process of aborting after the Abort button is pushed. • Aborting—The push task is executing the abort process. • Aborted—The push task has been successfully aborted. All changes made on all targeted devices are rolled back and the devices retain their original state prior to the work order execution. • AbortFailed—The push task failed to abort due to a failure of a device rollback process. • LockingResource—The state when the push task locks all necessary resources. • LockResourceFailed—The push task failed to lock all necessary resources. You can restart the work order in this state.
Start time field	The server start date and local time for the push task.

End time field	<p>The end time is the server local time when the following conditions occur for this push task:</p> <ul style="list-style-type: none"> • The work order finished successfully and paused. • A failed condition has been met and the work order stopped as a result of the failure. • The user manually stops a work order already in progress.
-----------------------	--

4. Click **OK**.

Delete a Fraud Protection List Push Task

A Fraud Protection List (FPL) push task can be manually deleted only if it is in the **PartialConfigured**, **NotScheduled**, **Aborted**, or **Committed** state.


1. Expand the **Fraud Protection Manager** slider and click **Fraud protection list**.
2. Click the **Device association** tab, and select the FPL push task from the **FPL push tasks** table and click **Delete**.
3. In the confirmation dialog box, click **Yes**.

Configure a Fraud Protection List Backup Schedule

You can schedule the automatic backup of Fraud Protection List (FPL) on a device to be run once, daily, weekly, or monthly.

Add a Fraud Protection List Backup Schedule

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Schedule** tab, click **Add Schedule**.
3. In the **FPL Archive Schedules** pane, complete the following fields:

Schedule drop-down list	<p>Select from the following options to set the type configuration backups for devices:</p> <ul style="list-style-type: none"> • Schedule—Select to schedule a date and time and make the configuration backup available on an on-demand basis. • On Demand—Select to make the configuration backup available on an on-demand basis. <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The parameters described below are unavailable if you choose this option.</p> </div>
Frequency drop-down list	<p>Select from the following options to set the frequency of configuration backups for devices:</p> <ul style="list-style-type: none"> • None—Select to not repeat a scheduled backup.

	<ul style="list-style-type: none"> • Daily—Select to perform daily backups. • Weekly—Select to perform weekly backups. • Monthly—Select to perform monthly backups.
Schedule drop-down list	Select a start date using the calendar icon.
Start time drop-down list	Select a start time in a 24-hour cycle.

4. Click **Add**.
5. In the **Select Device** dialog box, choose the device or device group in the **Managed devices** pane for which you want to schedule a backup, and click **Add** to move it to the **Targeted devices** pane.
6. Click **OK**.
The targeted device for scheduled configuration backups appears in the **Devices** table.
7. Click **Apply** to complete the backup schedule for the device.

Manage the Fraud Protection List Archive

Use the following tasks to specify a Fraud Protection List (FPL) backup schedule for one or more devices and use FPL archive file to restore or seed a new FPL.



Note:

Refer to Security Manager **Applications** tab if you need to change your user group privileges to allow you to manage the telephony fraud archive.

Edit a Fraud Protection List Backup Schedule

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Schedule** tab, select a backup schedule and click **Edit Schedule**.
3. In the **Edit Schedule** dialog box, you can modify some of the following fields:

Schedule check-box	Click to schedule the FPL backup for a device. If you uncheck the box, the FPL backup is no longer automatically performed and the other fields are not accessible.
Source field	(Read-only) The source device from which the FPL is backed up.
Frequency drop-down list	Select from the following options to set the frequency of configuration backups for devices: <ul style="list-style-type: none"> • None—Select to not repeat a scheduled backup. • Daily—Select to perform daily backups.

	<ul style="list-style-type: none"> • Weekly—Select to perform weekly backups. • Monthly—Select to perform monthly backups.
Schedule drop-down list	Select a start date using the calendar icon.
Start time drop-down list	Select a start time in a 24-hour cycle.

4. Click **OK**.

Backup a Fraud Protection List Now

You can backup a Fraud Protection List (FPL) when ever you want, on-demand.

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Schedule** tab, select a backup schedule and click **Back Up Now**.

Restore a Fraud Protection List Backup

The Archive tab displays all of the FPL files that have been archived, whether manually, or as a result of a scheduled backup.

Note:

The purge policy or existing Fraud Protection List (FPL) backups are not affected when a backup is restored for a device.

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Archive** tab, select a backed up FPL file from the **FPL Archive File** table, and click **Restore**.
3. In the confirmation dialog, click **Yes** to restore the backed-up configuration.

View the Fraud Protection List Backup Schedule

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Schedules** tab to view the following columns for the Fraud Protection List (FPL) archive schedules for different Network Functions (NFs):

Network function	The Network Function (NF) to which the device belongs.
Source	The name of the NF target device(s) or device group that needs to be archived. The backup function retrieves a current FPL from a device specified in the FPL configuration.
Frequency	The scheduled backup frequency: None , Daily , Weekly , or Monthly .
First scheduled	The time the FPL is scheduled to be backed up and its frequency.

Last run time	The last time a scheduled FPL backup occurred.
Object ID	(Hidden) The internal database object identifier.

Search the Fraud Protection List Archive

Use this task to search the FPL archive for a list of existing Fraud Protection List (FPL) archive (backup) files.

Refer to the [Fraud Protection Manager Search Filters](#) section for more information on filtering when you use a search criteria.

1. Expand the **Fraud Protection Manager** slider and click the **Archive** folder in the navigation pane.
2. Click the **Archived FPL** tab.
3. In the **Archived FPL** tab, click **Search**.
4. In the **Schedule search** dialog box, complete any of the following fields to create a search criteria:

FPL field	The user-defined FPL name.
Source field	The source IP address of the device belonging to the FPL.
Hardware version field	The hardware version of a device belonging to the FPL.
Software version field	The software version of a device belonging to the FPL.
Start backup date field	Click the calendar icon to select the start date range for when a configuration was backed up to the configuration archive.
End backup date field	Click the calendar icon to select the end date range for when a configuration was backed up to the configuration archive.

5. Click **OK**.

Delete a Fraud Protection List Backup Schedule

1. Expand the **Fraud Protection Manager** slider and click **Archive**.
2. Click the **Schedule** tab, select a backup schedule and click **Delete**.
3. In the confirmation dialog box, click **Yes**.

The backup schedule for the device is deleted, the backups for the device cease and the existing archive for the device remains until the purge policy initiates.

Configure Fraud Protection List Purge Policies

You can specify an automatic Fraud Protection List (FPL) archive purge policy to define the number of FPL backup configurations to store per device and create a purge schedule for devices or device groups.

Create a Fraud Protection List Purge Policy

A purge policy must be selected and configured to have Oracle Communications Session Element Manager automatically delete Fraud Protection Lists (FPLs).

The Oracle Communications Session Element Manager plugin service provides the archive FPL name prefix for the archive FPL file name. The archived FPL files are kept in the following Oracle Communications Session Delivery Manager server folder directory:

AcmePacket/NNCArchive/FPL/Archive

 **Note:**

The archived FPL file for each device uses the device IP address in the directory path.

1. Expand the **Fraud Protection Manager** slider and click **Purge Policy**.
2. In the **Purge policy** tab, complete the following fields:

Fraudulent Archive Purge Policy section	<p>Please choose purge policy radio-button options—Select one of the following purge policy options:</p> <ul style="list-style-type: none"> • Policy 1—Total Number of back-up FPLs that are allowed to be stored per device. • Policy 2—Back-up FPLs for devices are purged on a daily, weekly or monthly basis.
Policy 1 section	Total number of backups to store per device —Enter a numerical value between 0 - 10.
Policy 2 section	<p>Enter values for the following fields:</p> <ul style="list-style-type: none"> • Deleting daily backup older than days—Enter a numerical value between 0 - 10. The default is 4 days. • Deleting weekly backup older than weeks—Enter a numerical value between 0 - 10. The default is 4 weeks. • Deleting monthly backup older than months—Enter a numerical value between 0 - 10. The default is 4 months.

3. Click **Apply**.

Purge Fraud Protection Lists On-Demand

You can select the purge policy you set earlier or target all backed up Fraud Protection Lists (FPLs) on a device or group. You can select multiple devices or multiple groups to purge at one time.

1. Expand the **Telephony Manager** slider and click **Purge Policy**.
2. Click the **Operation** tab and complete the following fields:

Fraudulent archive purge policy section	Select from the following scope options for the purge: <ul style="list-style-type: none">• Select Purge all archived configuration to purge all FPL files associated with selected device(s) or device group(s).• Select Purge per policy to purge selected devices according to set purge policy.
--	---

3. Select the NF folder or device that you want to purge from the **Managed devices** table, and click **Add**.

The NF folder or device appears in the **Targeted devices** table.

4. Repeat the previous step to select more NF folders or devices that you want to purge.
5. Click **Purge**.