Oracle® Communications Session Element Manager

User Guide for the Enterprise Edge and Core Plug-in

Release 17.0
F52428-04
April 2024

ORACLE

Oracle Communications Session Element Manager User Guide for the Enterprise Edge and Core Plug-in, Release 17.0

F52428-04

Contents

3 Configuration Manager

4 Configure and Apply Global Parameters to Devices

5 Configure and Apply Software and Bootloader Upgrades to Devices

6 View Work Order Information

7 Use an Offline Configuration for a Device Cluster

10 Dashboard Manager

11 Performance Manager

A Performance Group Reference

B Session Element Manager Traps

About This Guide

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

Related Documentation

Table 1 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 2 Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • 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	Provides the following installation information: • 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	Contains information about the administration and software configuration of the SDM feature support new to this release.

Table 2 (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Security Guide	Provides the following security guidelines: • 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	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.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing 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.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.
   - For non-technical issues such as registration or assistance with My Oracle Support, select `2`.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

This section provides a revision history for this document.

Date	Revision
April 2022	Initial Release.
October 2022	Includes updates for the SDM 9.0.1 Release.
April 2023	Includes updates for the SDM 9.0.2 Release.
April 2024	Includes updates for the SDM 9.0.3 Release.

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.

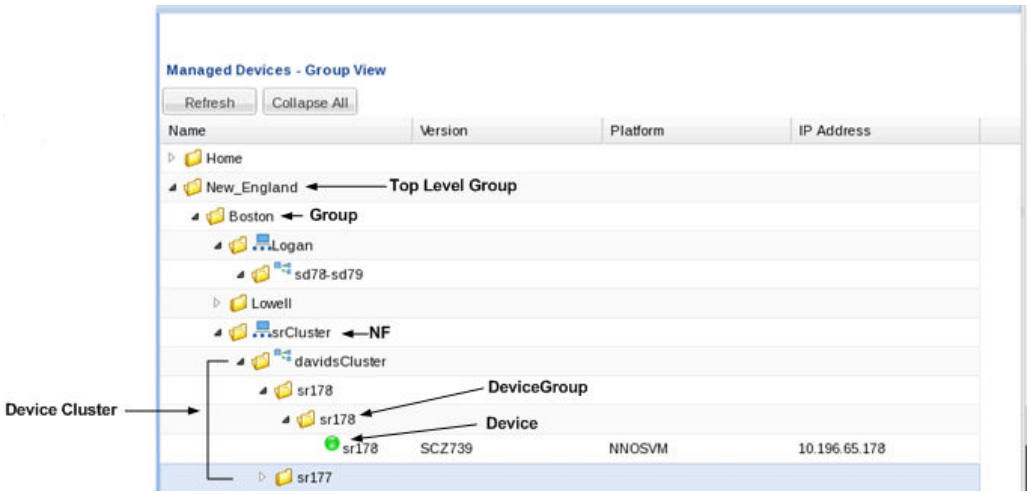
Session Element Manager Parts

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. The following illustration shows device groups and their associated NF devices.



Device cluster

A network function (NF) device cluster containing one or more groups that contain a device, a device cluster, or a high availability (HA) pair can be provisioned by using an offline configuration. An offline configuration template is used to efficiently target multiple individual devices (with the same software version and platform) so that you can quickly change their parameters with specific values.

Device group

A device group can contain or group NFs and devices.

> **Note:**
>
> Device groups can have polices applied which extend the device group characteristics, such as a cluster group.

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, high-availability (HA) pair or device cluster. A complex NF can consist of device groups that further define topological constructs and complex structures for device containment.

Offline Configuration

A common, top-level offline configuration template can be used to provision network function (NF) device cluster containing one or more groups that contain a device or a device high availability (HA) pair. An offline configuration can be created by making a copy of an existing configuration, packaged configuration, managed device configuration, or by selecting a schema from a supported software model.

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 9.0.3* 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 9.0.3* for the file name of your product plugin, and the *Oracle Communications Session Delivery Manager Administration Guide* for product plugin upload and installation instructions.

About Session Element Manager

The Oracle Communications Session Element Manager has the following sliders:

- **Dashboard Manager**—The dashboard summary view of at-a-glance status and key performance indicators for your managed devices.
- **Device Manager**—Use this slider to simplify the management of small to large networks of devices.
- **Security Manager**—Use this slider to configure any security privileges that are specific to Oracle Communications Session Delivery Manager and the Oracle Communications Session Element Manager product plugin. See the *Security Manager* chapter in the *Oracle® Communications Session Delivery Manager Administration Guide* for more information.
- **Configuration Manager**—Use this slider to do the following:
  - You can select from distinct configuration view styles that display a hierarchical view of infrastructure elements and their physical and logical components (for example, physical interface, virtual interface, realm, signaling service, session agents, and so on).
  - View the local configuration, change the configuration and push these changes to a device.

  - Create Golden Configuration, compare configuration of target devices with the Golden Configuration. Edit, download, purge comparison reports.
  - Use the **Global Parameter**, **Offline Configurations**, and **Reusable Modules** folder nodes to make configuring devices easier and manage software for multiple networks.
  - Use the features in the **Configure archive** folder node to perform automated and manual configuration backup for a device and restore configurations to a device from the archive.
- **Fault Manager**—View events, alarms, and trap summary data. See the *Fault Manager* chapter in the *Oracle® Communications Session Delivery Manager Administration Guide* for more information.
- **Performance Manager**—View SNMP, IP, environmental and other performance statistics collected from product devices.

Information for Oracle Enterprise Session Border Controller Users

The Oracle Communications Session Element Manager (SEM) supports using the Oracle Enterprise Session Border Controller (E-SBC) with all of the SEM managers.

From the SEM GUI, you can launch the E-SBC login page and perform operations on the E-SBC except for loading the E-SBC configuration when the selected E-SBC is operating in the Basic Mode.

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.

Information for Oracle Enterprise Communications Broker Users

The Oracle Communications Session Element Manager (SEM) supports using the Oracle Enterprise Communications Broker (ECB) with the full functionality of the SEM Dashboard, Device, Performance, and Fault managers. In the SEM Configuration Manager, SEM supports only the auto-backup functionality for the ECB.

From the SEM GUI, you can launch the ECB login page and perform operations on the ECB.

The SEM does not support:

- Loading the ECB configuration with the Configuration Manager
- Using the ECB in Report Manager and Route Manager
- Adding for modifying user group privileges for the ECB in Security Manager

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.

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.

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.
- **Bulk Device Deployment**—Add, remove, and manage devices and bulk device deployments 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.

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

As of Oracle Communications Session Element Manager Release 9.0, 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 SBCbased NF can be composed of two SBC instances running as a HA pair.

Oracle Enterprise Edge and Core 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 can select for your Oracle Enterprise Edge and Core Plug-in.

Product Category	NF Type	Component Devices
Enterprise Edge & Core	ESBC	Standalone Oracle Enterprise Session Border Controller (ESBC) device
	ECB	Standalone Oracle Enterprise Communications Broker (ECB) device
	Device Cluster	High-Availability (HA) device pair of the component devices listed above.

Add a Network Function with Devices

Use this task to add a network function (NF) with devices to the default **Home** group or a group that you created. Once the NF is added successfully, the Oracle Communications Session Element Manager plug-in is able to communicate with the devices in the NF.

Pre-requisite: If you are not using the default **Home** group to add an NF, you must specify a group for the NF.

1. Expand the **Device Manager** slider, and click **Devices**.
2. In the **Managed Devices - Group View** pane, select a group, and click **Add**.
3. In the **Select Network Function Type** dialog box, click the element manager (EM) product plugin category from the **Categories** table that manages your devices.
4. In the **Network Function Type** drop-down list, select from the following NF types:
   - **Device**—A NF that contains a single standalone device or device high-availability (HA) pair.
   - **Device Cluster**—An NF that contains a device cluster that shares a common, top-level offline configuration template.

   > **Note:**
   >
   > Oracle Communications Report Manager does not currently support device clustering.

5. Click **Continue**.
6. In the **Add Network Function: Device** dialog box, complete the following fields:

Network Function Name field	The Network Function (NF) name that you want to use for the device(s) that you are configuring.
Primary IP address/ FQDN field	The primary IP address or FQDN for this device.
Secondary IP address/FQDN field	The IP address or FQDN for the second device, if this device is part of an HA pair. Both FQDNs for the HA pair devices must be mapped to the corresponding IP addresses in the /etc/hosts file where OCSDM is installed.
User Name field	The device user name.
User Password field	The device password.
LI encryption password field	(Hidden) The Lawful Intercept (LI) encryption password for the LI configuration. This field appears if the LI administrator is logged into Oracle Communications Session Delivery Manager. This parameter is not available for the Enterprise Edge and Core plug-in at this time.

	Note: Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.
SNMP agent mode drop-down list	Select the SNMP version number that the SNMP agent supports and click **Load**. Valid versions are **v1**, **v2** and **v3**. If you select **v3**, authentication fields for SNMP version 3 appear. See below for more information about these fields. When you add a device, you must specify whether to manage the device using SNMPv1, SNMPv2, or SNMPv3. The SNMP version cannot be changed for an existing device once it is added unless the device is removed and added again later.
SNMP port field	The SNMP port number. The default SNMP port number is 161.
SNMP community name field	The SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. This field applies only to SNMP version 1 and 2. The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the **ip-addresses** parameter found in the **configure terminal**, **system**, **snmp-community** element. For more information, see the device product documentation.
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **SHA**—Secure hash algorithm (SHA-1). • **MD5**—MD5 hash algorithm. • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **DES**—Data encryption standard algorithm (DES) for the encryption of electronic data.

	• **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**
SNMPv3 privacy password field	The SNMP version 3 privacy password.

7. Click **Apply**.

   The NF and its associated device(s) or the NF with the associated device(s) appear in the **Managed Devices** table. The **Managed Device** table shows the IP address or the FQDN depending on the details added by the user in the **Device Manager**.

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. You can access the web GUI using the IP address or FQDN. When you launch a managed device using FQDN, the FQDN to IP mapping is looked up in the DNS. If the FQDN to IP mapping is present in the DNS, the web GUI can be accessed using FQDN. The web GUI access using IP address searches either the /etc/hosts or the DNS.

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:

> **Note:**
>
> You cannot edit the NF name or its device(s) IP address(es).

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.

User Name field	The new device user name.
User Password field	The new device password.
LI encryption password field	(Hidden) The Lawful Intercept (LI) encryption password for the LI configuration. This field appears if the LI administrator is logged into Oracle Communications Session Delivery Manager. This parameter is not available for the Enterprise Edge and Core plug-in at this time. **Note:** Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.
SNMP community name field	**Note:** This field applies only to SNMP version 1 and 2. Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. **Note:** The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the **ip-addresses** parameter found in the**configure terminal, system, snmp-community** element. For more information, See the device product documentation for more information.
SNMP port field	The SNMP port number. The default SNMP port number is 161.
SNMP community name field	**Note:** This field applies only to SNMP version 1 and 2.

	Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. **Note:** The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the **ip-addresses** parameter found in the**configure terminal**, **system, snmp-community** element. For more information, See the device product documentation.
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **SHA**—Secure hash algorithm (SHA-1). • **MD5**—MD5 hash algorithm. • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **DES**—Data encryption standard algorithm (DES) for the encryption of electronic data. • **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**
SNMPv3 privacy password field	The SNMP version 3 privacy password.
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.

Remove a Network Function

When you remove an NF, all references to the NF in Configuration Manager, Device Manager, Fault Manager, Report Manager, Route Manager, Security Manager and Performance Manager are removed.

> **Note:**
>
> You cannot remove an NF during a configuration update or if the NF 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, click the NF folder you want.
3. Click **Remove**.
4. In the **Remove device** dialog box, click **Yes**.

   The NF (folder) and its device(s) are removed from the group hierarchy.

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.

Reboot a Device

> **Note:**
>
> You must have the appropriate administrator permissions assigned to reboot a device.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the device you want to reboot, and click **Admin**, **Reboot**.

3. In the **Confirm** dialog box, click **Yes**.

> **Note:**
>
> The targeted device is rebooted.

4. Once you see the reboot process finish in the **Progress** dialog box, click **Close**.
5. In the **Reboot Device** dialog box, click **OK**.

> **Note:**
>
> This dialog box confirms that the reboot process has completed successfully.

Synchronize System Alarms with a Device

If the NF has an HA device pair, when you synchronize one device the other device in the pair is also synchronized.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the device you want to synchronize with system alarms and click **Admin**, **Synchronize alarms**.
3. In the **Synchronize alarms** dialog box, click **Yes**.
4. In the Information dialog box that displays, click **OK**.

Manage a Device Configuration in a Network Function Device Cluster

When new device variables are added to an offline configuration (in Configuration Manager) that NF device cluster devices use, you must configure each device in a device cluster with its needed device parameters.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, navigate to an NF device cluster device and click **Configure**.
3. In the **Configure data variable for....** dialog box, enter the required parameter(s) for the data variables for which you are prompted.
4. Click **Finish**.

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.

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 Hardware Details for a Network Function Device

You can find the following component inventory data for a NF device, such as chassis, CPU, memory, and so on.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Get Information**, **Show details**.
3. In the **Hardware** tab, the following columns display for NF standalone devices, or an NF HA pair of devices:

Index	(Hidden) The number assigned to each component of the device.
Description	The text description of the physical entity.
Vendor type	The vendor-specific hardware type of the physical entity. **Note:** This value is different from the definition of MIB-II sysObjectID.
Contained in	(Hidden) The index number in which this hardware component is contained.
Class	The enumerated value that indicates the general hardware type of this physical entity.
Name	Textual name of this physical entity. Name of the component as assigned by the local device.
Hardware Rev	The vendor-specific hardware revision string for the physical entity.
Firmware Rev	The vendor-specific firmware revision string for the physical entity.
Manufacturer	The name of the manufacturer of this physical entity.
Model Name	The vendor-specific model name identifier string associated with this physical entity.
Is FRU	This indicates whether this physical entity is considered a field replace unit (FRU) by the vendor.
Serial Number	The serial number of the chassis or module. Serial number information is pulled from a physical device through SNMP. Virtual devices return a value of **N/A**.
Object ID	(Hidden) The database object ID for this device.

View Software Details for a Network Function Device

The following boot parameters are displayed for Oracle Communications session delivery product devices:

- The software image and where the image is booted for this NF device (on an external device or internal flash memory).
- The type of software entity being booted.
- Status of that software entity.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Get Information** and then click **Show details**.
3. In the **Device details** pane, click the **Software** tab. The boot table and **Backup** table columns display for NF standalone devices, or an NF HA pair of devices:

Current configuration version field	The saved version number of the current configuration image.
Running configuration version field	The saved version number of the configuration currently running on the Oracle Communications session delivery product.
Index column	The number assigned to each software image on the device.
Description column	The software image name, device location, IP address or other unique identifiers. For example: • host address/image name (boot image) 10.0.1.12/sd121p3.gz • boot from flash0/image name (boot image) /tffs0/sd121p3.gz • bank0:date time (boot loader) bank0:06/13/2005 10:58:25
Type column	The software entity type. Values are: • **bootImage** • **bootLoader**
Status column	This column describes whether the software image is currently used or previously used.
Backup column	The Oracle Communications Session Delivery product device can save an existing configuration into a single backup file. Backups are created as gzipped tar files in a .tar.gz format. They are stored in the /code/bkups directory on the Oracle Communications session delivery product device.
Object ID column	(Hidden) The database object ID for the device.

View License Details for a Network Function Device

Use this task to show product devices that have an applied license key.

1. Expand the **Device Manager** slider and click **Devices**.

2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Get Information** and then click **Show details**.
3. In the **Device details** pane, click the **License** tab. The following field and table columns display:

License Key column	The license number.
Capacity column	The maximum number of simultaneous sessions allowed by the device for all combined protocols.
Install Date column	The installation time and date when the software was installed on the device. **N/A** appears if a license is not enabled.
Begin Date column	The beginning time and date when the software was licensed on the device. **N/A** appears if a license is not enabled.
Expire Date column	The end time and date when the software license expired on the device. **N/A** appears if a license is not enabled.
Protocol Names column	All protocols licensed for this device. Values are: SIP, MGCP, and H.323.
Feature Names column	The following features can be licensed for this device: • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG) • ACC—Enables Oracle Communications session delivery product devices to create connections, and send CDRs to one or more RADIUS servers). • High Availability (HA)
Object ID	(Hidden) The database object ID for this device.

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
Configuration Manager

Use Configuration Manager to load, configure, apply, and save a configuration on Network Function (NF) devices.

The Configuration Manager provides the following tools to add and manage configurations on managed devices.

> **Note:**
>
> For Oracle Enterprise products, Configuration Manager supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB) and only for selected operations. See "Information for Oracle Enterprise Session Border Controller Users" and "Information for Oracle Enterprise Communications Broker Users."

Tools	Operations
Devices	• Global settings—configure system, redundancy, management, IWF, security, routing, and services
Configuration tools	• Global parameters—add and manage global configurations • Offline configurations—add and manage offline configurations • Reusable modules—add and manage reusable configuration modules
Configure archive	• Schedule—add an archive schedule to managed devices • Archive configuration—add and manage archive configurations • Administration—configure archive purge policy and apply to selected devices

Associate Devices with Session Element Manager

The devices that were added previously in Device Manager can now be associated with the Oracle Communications Session Element Manager, so that it can manage and provide full **fault, configuration, accounting, performance, security** (FCAPS) support for these devices.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Configuration Manager** slider, and select **Devices**.
2. In the **Managed Devices** table, click **Add devices**.
3. From the **Device list** table, expand the Network Function (NF) folder hierarchy, select the device from the devices that want to associate with OCSEM, and click **Add**.

   The entire NF folder hierarchy, including the NF appears in the **Targeted devices** table.
4. Click **OK**.
5. In the success dialog box, click **OK**.

   The device is now associated with OCSEM.

Now that the device(s) are associated, they are polled for health statistics and configurations can be loaded and managed for these device(s).

Upload a Configuration Schema for a Device

You can use this task to manually upload the configuration schema when the Oracle Communications Session Element Manager cannot get the configuration schema (XSD file) from the device.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

All software release configuration information is modeled and maintained in a valid configuration schema for a device so that it can be managed by OCSEM. Most often, a software release schema is matched for a device, which is required so that the device can be assigned in Configuration Manager. If a software release is not found, OCSEM attempts to get the configuration schema directly from the device (in recent device releases, the configuration schema is packaged with the release image), and put it in the database local schema repository.

> **Note:**
>
> If the schema for a device does not exist for a software release, the device can be added to Device Manager but cannot be managed by OCSEM.

1. On the menu bar, select **Tools**, **Upload configuration schema file**.
2. In the **Upload configuration schema file** dialog, select the product plug-in category (for example, **SP Edge & Core**) from the **Categories** table for the product plug-in.
3. Click **Browse**, and navigate to a valid configuration schema file on your system.
4. In the **File Upload** dialog, select the configuration schema you want to upload, and click **Open**.

5. In the **Upload configuration schema file** dialog, click **Upload** to start the upload process.
6. In the success dialog, click **OK**.

Load the Configuration of a Local Device to Configure a Device

A copy of the configuration on a network function (NF) is loaded on the Oracle Communications Session Element Manager application database so that this configuration can be viewed, modified, and validated with minimal interaction with the NF. You must load the configuration to view the configuration and expand it in the navigation tree. After the configuration is loaded, you can check if the configuration copy in the database is current with the configuration version of the device. If the configuration version is not current, the Oracle Communications Session Element Manager application retrieves the latest configuration from the device. This on-demand loading of a configuration ensures that the local copy of the configuration and the configuration on the device are always synchronized.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Devices**.
2. In the **Managed Devices** table, expand the folder hierarchy, and click the NF folder to expand its device(s).
3. Click any device you want to load, and click **Load**.
4. In the success dialog, click **OK**.

   The NF configuration is loaded.

Navigate Configuration Manager Views

You can use different Configuration Manager views to navigate the top-level configuration elements of your device by selecting the configuration element and its associated parameters, which appear in the display pane. You can switch between the following views at any time during your session.

Select from the following drop-down list views below the **Configuration Manager** slider:

> **Note:**
>
> For Oracle Enterprise products, configuration views supports only the Enterprise Session Border Controller (ESBC).

- **Default view**—The top-level configuration elements are grouped into logical, function-specific Oracle Communications Session Delivery Manager category labels that are grouped for a required configuration task and its associated parameters.

- **CLI view**—The top-level elements display in the active product device folder as they appear and are grouped in the device CLI. The product device configuration labels are listed according to their corresponding CLI parameter format.
- **List view**—The top-level elements display in an alphabetically-ordered list, and in a CLI parameter format. There is no special grouping as there is with the other two views.

In the **CLI view** and **List view**, you can see more element attribute columns by checking the **Retrieve all attributes** check box. Next, when you select the column arrow menu to access element attribute column selections, all display. See the *Customize the Display* section in the *Overview* chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.

> **Note:**
>
> If the **Retrieve all attributes** check box is checked, it stays checked for the duration of the session.

Discover a Device Not Appearing in Configuration Manager

Use this task if a device was added in Device Manager, and this device is not visible in Configuration Manager (even after clicking **Refresh**).

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Device Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, click **Refresh**.
3. Return to Configuration Manager to continue your configuration for the device that now appears.

Manage Device Configurations

View Managed Devices

When you want to view the details about the configuration of a managed device, use the Devices object in Configuration Manager to display a list of managed devices with the corresponding configuration parameters.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Configuration Manager** slider and select **Devices**.
2. In the **Managed Devices** table, the following columns display:

Name	The group, subgroup, network function (NF), and device that belongs to each NF. The grouping structure of the NF and its devices is determined by the Session Delivery plug-in.
Software Version	The full software release version, including patch number of the NF HA device pair or standalone device.
Platform	The device hardware platform.
Device Configuration Version	The configuration version running on the device. This version number changes and increases each time the device configuration is modified.
Loaded Configuration Version	This is the configuration version number that indicates the last uploaded version of the configuration from the device and stored in the database. This number changes each time a new configuration is uploaded form the device.
Last Operation	The last operation performed on the NF or its components.
Status	The status of the last device operation.
Status Change Time	The time of the last device operation.
Pending Changes	The number of pending changes for the device.
IP Address/FQDN	The device IP address or FQDN of the device. The **Managed Device** screen under **Configuration Manager** displays the IP address or FQDN depending on the details added by the user in the Device Manager.
Target Name	(Hidden) The device target name.
Category	(Hidden) The element manager (EM) plug-in product vendor category.

Component	(Hidden) The available NF component delivered by the EM plug-in product vendor category.
Vendor	(Hidden) The plugin vendor to which the devices belong.
DeviceConfigId	(Hidden) The identity provided by the plugin. For example, the device identity for the plugin is its target name.
Object ID	(Hidden) The internal database object ID.
Group ID	(Hidden) The parent group ID.
Offline Configuration	(Hidden) The name of the offline configuration for the NF device cluster that associates with it. This offline configuration is used to initiate devices (to be added later) to this NF device cluster.
Synchronized Mode	(Hidden) The synchronized mode column displays if the devices in a scalability group (For example, "Device Cluster" for the plugin) have their individual configurations kept in synchronicity with the configuration defined in the offline configuration as it changes over time.
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.

Update a Device Configuration

Pre-requisites: Before you update a device configuration you must first load it in Configuration Manager. See the Load the Configuration of a Local Device to Configure a Device section for more information.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click the **Devices** folder.
2. In the **Managed Devices** table, expand the folder hierarchy, select a network function (NF) device, and click **Update**.
3. In the dialog that appears, select from the following options to update the device configuration:

> **Note:**
>
> The first two options are only available if there are pending changes to be saved. The third option is only available if there are no user changes, and there is a saved configuration pending activation.

Save & activate configuration	(Default) Click to save the configuration and make the current configuration on the device the running configuration.
Save configuration	Click to save the current configuration changes to the device.
Activate configuration	Click to make the current configuration the running configuration.

View Device Configuration Changes

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click the **Devices** folder.
2. In the **Managed Devices** table, expand the folder hierarchy, select a network function (NF) device, and click **View Changes** to display a list of all configuration changes made for this device.
3. In the **Configuration Changes** pane, the changes made by the current user appear for the NF device in the **LCV** (Local Configuration View) table. The following table describes the LCV columns:

User	The name of the user who performed the configuration changes.
Type	The CLI parameter name.
Name	The configuration element instance name.
Operation	The result of the parameter change that occurred on the configuration. Valid values are **created**, **modified**, and **deleted**.
Time changed	The time when the configuration changed, which is not propagated yet to the device.

4. You can use the following actions in the **Configuration Changes** pane:

> **Note:**
>
> You must have the appropriate user privileges to perform actions in the **Configuration Changes** pane.

Refresh	Click to refresh the data in the view changes list.
Undo Changes button	Select a change row and click to undo selected changes.

Change Owner	Click to transfer the ownership of your changes to another user.
Update	Click to launch a dialog that is used to update the configuration with one of the following options: • (Default) Click **Save & activate configuration** to save the configuration and make the current configuration on the device the running configuration. • Click **Save configuration** to save the current configuration changes to the device. • Click **Activate configuration** to make the current configuration the running configuration. **Note:** This option displays depending on the changes that were saved.

Track Device Configuration Changes

Use this task to track changes that are made to device parameters.

Note:

For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click the **Devices** folder.
2. In the **Managed Devices** table, expand the folder hierarchy, select a network function (NF) device, and click **Get Inventory**.
3. In the **Configuration inventory** dialog that appears for the device, review the number of each type of configuration element.
4. (Optional) Click **Save to file**.
5. In the dialog that appears, click **OK** to download the information in the format of a comma-separated values (CSV) file to your system.

View Device Tasks

Note:

For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Configuration Manager** slider, and click the **Devices** folder.
2. In the **Managed Devices** table, expand the folder hierarchy, select a network function (NF) device, and click **View tasks**.
3. In the **Device tasks** table, you can view the device operations that are performed and if you select a device operation row, you can see logs for this device operation by clicking **View Log**.

Export Detailed Device Information from Configuration Manager

You can export network function (NF) device information to your local system, which allows data to be saved in a table-structured format for auditing or management purposes.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, expand the folder hierarchy, select an NF device, and click **View Changes**.
3. In the **Configuration changes** pane, click **Save to File**.
4. In the dialog, click **OK** to download the information in the format of a comma-separated values (CSV) file to your system.

Remove Device Association with Session Element Manager

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** table, click **Add devices**.
3. In the **Devices associated with Element Management** pane, expand the folder hierarchy in the **Targeted devices** table, and click the network function (NF) device you want to remove.
4. Click **Remove**.

   Your device is no longer associated with Oracle Communications Session Element Manager and appears in the **Device list** pane.
5. Click **OK** to apply the changes.

Golden Configuration

A golden configuration is a configuration version which can be used as a tool to maintain configuration integrity. Administrators can use the golden configuration as a master version to compare device configurations and report discrepancies.

Users belonging to the administrators and LIAdministrators group can create, edit, and delete the Golden configuration. Other users can create, view, download, and delete the configuration comparison report.

Prerequisites for Creating a Golden Configuration

As an Administrator user, you can create a Golden Configuration for a managed device by selecting the managed device, or by using an archived configuration, or an external file. Ensure that you have read this information before starting the procedure.

Creating a Golden Configuration Using Managed/Associated Device Option

If you are creating the Golden Configuration using the **Managed/Associated Device** option, ensure that the device is associated with the Oracle Session Element Manager. For more information, see Associate Devices with Session Element Manager. You can create the Golden Configuration uisng the **Managed Device** option for only such devices that are associated with the Session Element Manager.

Creating the Golden Configuration Using the Archived Configuration Option

If you are creating the Golden Configuration using the **Archived Configuration** option, make sure that the backup configuration is available for the associated device. The backup configurations can be seen under **Archive Configuration** under the **Configuration Manager** slider. For more information, see Add a Backup Schedule.

Creating the Golden Configuration Using the External Files Option

If you are creating the Golden Configuration using the **Upload External files** option, make sure that the file is an XML or Gzip file, with a valid file name - the file name cannot contain spaces and can only contain letters, numbers, an underscore, or a hyphen. The configuration file must be of the same plugin and same platform type as that of the Golden Configuration.

Creating the Golden Configuration

As a user belonging to the Administrator or LI administrator groups, you can create the Golden Configuration so that users can use it as a basline configuration and identify network discrepancies by comparing it with network function configurations.

You can create only one Golden Configuration per managed device. You can use this Golden Configuration later to compare with multiple other configurations of the same plugin type and platform type identical to the Golden Configuration.

For more information on getting things ready for creating the Golden Cofiguration, see Prerequisites for Creating a Golden Configuration.

1. Expand the **Configuration Manager** slider and click **Configuration Comparison**.
2. Click **Golden Configuration**.

3. In the **Golden Configuration** page, click **Create**.

Table 3-1 Comparing the Configuration Report

Field	Description
Golden Configuration Name	Name of the Golden Configuration. The name must be a valid name and unique name without any space characters. A valid name can contain only letters, numbers, an underscore, or a hyphen. No blank space(s) are allowed, and the name should not start with 'ID'.
Device Association - Associate device from managed device	Click to view the **Select Managed Device** dialog box which displays all devices added in SDM. Select any one device.
Configuration selection - Golden Configuration Seeded from:	Select the source to derive the Golden Configuration. You can select the configuration using any one of the three options: • **Managed/Associated Device**: The Golden Configuration is seeded from the running configuration of the associated device that you selected in the previous row. • **Archived Configurations**: Click this radio button to enable the **Archived Configuration** drop down list. **Note:** The **Archived Configuration** drop-down list is enabled only if you select the **Archived Configurations** radio button. The **Archived Configuration** drop down list displays a list of backup configurations of the associated device from the configuration archive. Select one backup configuration. • **Upload external files**: Click this radio button to enable the **Upload file** field. Click the browse button to select an XML or GZip file with a valid name. In the **Upload Configuration File** window, provide information for the **Category** and **Platform** fields. The Category and Platform values must match with that of associated device selected in the previous row. For information on the supported Plugins and Platform, see Supported Plugins and Platforms.

4. Click **Apply**.

The Golden Configuration for the selected managed device is created. You can view the list of Golden Configurations in the **Golden Configuration** page.

5. Hover the mouse pointer on any column header to select the sorting order, hide or show columns from the display.

Supported Plugins and Platforms

One of the options to create a Golden Configuration is using **Upload External Files**. This option requires you to provide information on the Plugin and Platform type associated with the external file that you upload.

Why Do We Need Plugin and Platform Information

When you create a Golden Configuration using the **Upload External Files** option, the uploaded configuration file does not contain details such as product type and platform. Hence, Plugin and Platform information must be added. In the uploaded configuration file, SDM cannot differentiate the product type. The list of Platforms and Plugins supported by SDM is given below:

Supported Platforms

This table lists supported platforms in SDM.

- AP4600
- AP4250

> **Note:**
> Only SP Edge and core platform

- AP4500
- AP6100
- AP6300
- AP6350

> **Note:**
> SP Edge, Enterprise Edge, and Core platform

- AP1100

> **Note:**
> Only Enterprise Edge and Core platform

- AP3900
- AP3820
- AP3800

> **Note:**
>
> Only SP Edge and Core platform

- NNOSVM
- NNOS

Supported Plugins

- Enterprise Edge and core
- SP Edge and core

Editing a Golden Configuration

As the Administrator, you can edit or overwrite an exisiting Golden Configuration.

1. Expand the **Configuration Manager** slider and click **Configuration Comparison**.
2. Click **Golden Configuration**.

   The Golden Configurations page displays a list of all existing Golden Configurations.
3. Select the Golden Configuration that you want to edit.
4. Click **Edit**.
5. In the **Edit Golden Configuration <name>** page, you can change the source of the Golden Configuration. However, you cannot change the name of the Golden Configuration and associated device fields. The process is identical to creating a new Golden Configuration.
6. Click **Update**.

Deleting Golden Configuration

As the Administrator user, you can delete a Golden Configuration.

Deleting Golden Configuration can be performed by the Administrator.

1. Click the **Configuration Manager** slider and click **Configuration Comparison**.
2. Click **Golden Configuration**.
3. In the **Golden Configuration** page, select the one that needs to be deleted.
4. Click **Delete**. Click **ok** to confirm.

Configuration Comparison

For more information, see:

1. Creating the Comparison Report
2. Viewing the Comparison Report
3. Downloading the Comparison Report
4. Deleting the Comparison Report
5. Setting the Purge Method for Comparison Reports

.

Creating the Comparison Report

Comparing device configuration with a Golden Configuration allows you to view discrepancies from the baseline, and create a comparison report.

Create a comparison report by comparing the Golden Configuration against a device configuration of the same Plugin and Platform type.

Make sure that a Golden Configuration has been created for the same Plugin and platform type of the device that you are about to compare.

1. Expand the **Configuration Comparison** slider.
2. Click **Compare Comparison**.
3. In the **Configuration Comparison Reports** page, click **Create**.
4. In the **Create Configuration Comparison** page:

Table 3-2 Fields in the Create Configuration Comparison Page

Field	Description
Comparison Report Name	Valid name of the configuration comparison report. A valid name can only contain letters, numbers, an underscore, or a hyphen. No blank space(s) are allowed, and the name must not start with `ID`.
Source	Select an existing source Golden Configuration against which the target configuration needs to be compared.
Target Configuration Selection	Target can be any one of these options: a device configuration, backup configuration or an external configuration file. • **Managed device**: The selected device must have an identical platform and plugin type as the source Golden Confguration. • **Archived configuration** displays only those backup configurations that match the platform and plugin type as that of the source Golden Configuration • **Uploaded external file** The external file must have an identical platform and plugin type as the source Golden Configuration.

5. Click **Apply**.

   The Configuration Comparison report is created.

Viewing the Comparison Report

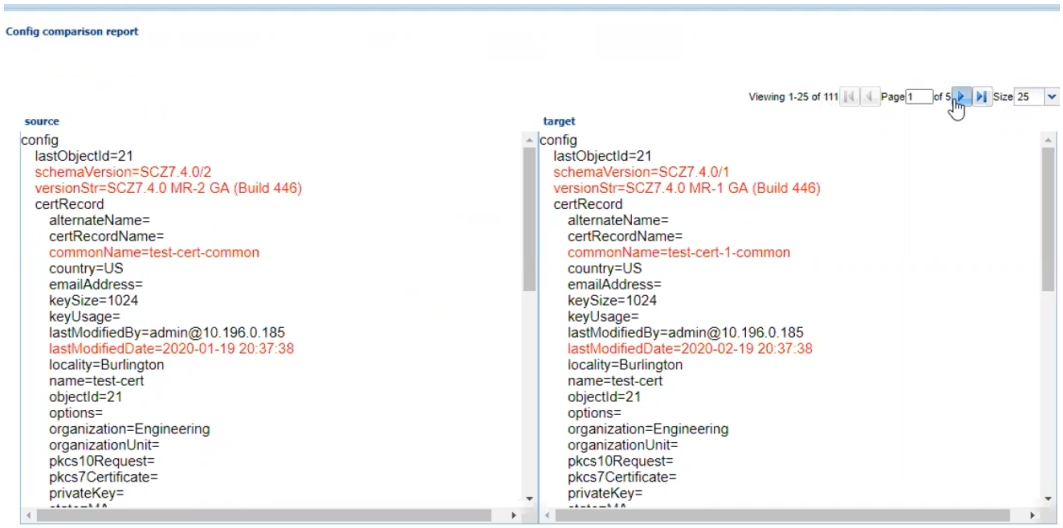
Viewing the comparison report shows the configuration differences between the source Golden Configuration and the taget configuration.

1. Expand the **Configuration Comparison** slider.

2. Click **Compare Comparison**.
3. In the **Configuration Comparison Reports** page, click the comparison report that you want to view.
4. Click **View**.

   The comparison report is shown in two-column mode highlighting the differences in red font.

Figure 3-1 View Comparison Report



5. Click **Back** to go back to the list of comparison reports.

Downloading the Comparison Report

You can download the Configuration Comparison Report for future reference.

1. Expand the **Configuration Comparison** slider.
2. Click **Compare Comparison**.
3. In the **Configuration Comparison Reports** page, select the report that you want to download.
4. Click **Download**.
5. When the system prompts you to download the report in compressed gzip file format, click **Yes**. Clicking **No** allows you to download the report in a PDF format.

   The comparison report file that you download contains the following information:

   - Report name
   - Source Configuration
   - Target Configuration
   - Platform
   - Plugin type

- Source Software version
- Target Software version
- Report Generated Date
- Owner

Deleting the Comparison Report

You can delete the Comparison Reports that you no longer require or those that are not relevant anymore.

1. Expand the **Configuration Comparison** slider.
2. Click **Compare Comparison**.
3. In Configuration Comparison Reports, click the report that you want to delete.
4. Click **Delete**.

   On confirmation, the report is deleted from SDM

Setting the Purge Method for Comparison Reports

You can purge comparison reports in two ways: auto purge or manual method.

1. Expand the **Configuration Comparison** slider.
2. Click **Compare Comparison**.
3. Expand the **Configuration Comparison** slider.
4. Click **Purge**.
5. In the **Purge Comparison Reports** page:

Table 3-3 Fields in the Purge Comparison Reports

Field	Description
Auto Purge	Select this method to purge comparison reports automatically by the Purge task that runs everday at 1 A.M. All reports that are older than the auto-purge interval are purged.
Enter the number of days to keep the comparison reports	Set the auto purge interval in terms of days (24 hours day). By default, the purge interval value is 2 days. You can set the purge interval value as required, but the value must be greater than 2 days. If you set the purge interval as 4 days, then all reports that were saved 4 days before today are purged today by the Purge task.
Manual Purge	Select this method to manually purge the reports. Select the **From** date and **To** date. Do not select today, yesterday, or a future date. This is because the default purge interval is 2 days.

6. Click **Apply**.

Based on the method that you select, reports that qualify for purging are purged from SDM.

Manage the Configuration Archive

Depending on your user privilege level, or privileges set for the User Group to which you belong, you can manage the configuration archive.

A configuration can exist on every node of a device cluster. When a configuration file is pulled from a device by a node, the file is sent to all cluster nodes. See *Security Manager* in the Oracle Communications Session Element Manager if you need to change your privileges to allow you to manage the configuration archive.

> **Note:**
>
> For Oracle Enterprise products, the Configuration Archive supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

> **Note:**
>
> When R226 compliance is set as enabled upon installation, the OCSDM hides LI and SIPREC attributes, however, they still exist in the datadoc.

Add a Backup Schedule

Use this task to schedule automatic configuration backup for a device or a device group to run once, daily, weekly, or monthly automatically. You can also configure a backup to run on demand. The following actions occur when you create a backup:

- A new directory is created for each device using its device name in the **AcmePacket/ ConfigBackups** directory.
- An entry is added to the database for the configuration file.
- The set purge policy is applied.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. On the **Configuration Manager** slider, select **Configure archive**, **Schedules**.
2. In the **Schedules** pane, click **Add schedule**.
3. In the **Add Schedules** tab, complete the following fields:

Schedule drop-down list	Select from the following options to set the type configuration backups for devices: • **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. **Note:** The parameters described below are unavailable if you choose this option.
Frequency drop-down list	Select from the following options to set the frequency of configuration backups for devices: • **None**—Select to not repeat a scheduled backup. • **Daily**—Select to perform daily backups. • **Weekly**—Select to perform weekly backups. • **Monthly**—Select to perform monthly backups.
Start date 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 the **Devices** tab.
5. Click **Add**.
6. In the **Select Device** dialog, 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.
7. Click **OK**.

   The targeted device for scheduled configuration backups appears in the **Devices** table.
8. Click **Apply** to complete the backup schedule for the device.

Restore a Configuration Backup

The purge policy or existing configuration backups are not affected when a backup is restored for a device.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. On the **Configuration Manager** slider, select **Configure archive**, **Archive configuration**.
2. Select a backed up configuration from the table, and click **Restore**.
3. In the confirmation dialog, click **Yes** to restore the backed-up configuration.

View a Backup Schedule

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. On the **Configuration Manager** slider, select **Configure archive**, **Schedules**.
2. In the **Schedules** pane, Session Element Manager displays the following columns:

Parent Group	The parent network function (NF) group that is provided by the user or Oracle Communications Session Element Manager plugin.
Source	The name of the NF target device(s) or device group that needs to be archived.
Frequency	The scheduled backup frequency.
First scheduled	The first time the schedule is started.
Last run time	The last time a scheduled backup was done.
Platform version	The current hardware version. If it is a device group, the value is N/A.
Software version	The current software version. If it is a device group, the value is N/A.

Rename a Configuration

You can rename any backed up configuration file to make its name more meaningful. The actual file name on the system does not change and continues to adhere to the set file naming policy. This configuration name only appears within the context of Oracle Communications Session Element Manager.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. On the **Configuration Manager** slider, select **Configure archive**, **Archive configuration**.
2. In the **Archive configurations** pane, select the configuration you want to rename, and click **Rename**.
3. In the **Name** field, enter a new name for the configuration.
4. Click **OK**.

   The alias name for the configuration appears in the list of archive configurations instead of its actual configuration file name.

Manage Purge Policies

You can select a purge policy for devices or device groups. You can customize the purge policy to define the number of backup configurations to store per device, to configure the purge schedule for devices or device groups, and to purge them immediately.

> **Note:**
>
> For Oracle Enterprise products, purge policies support only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Purge Configurations On-Demand

You can select the purge policy you set earlier or target all backed up configurations on a device or group. You can select multiple devices or multiple groups to purge at one time.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. On the **Configuration Manager** slider, select **Configure archive**, **Administration**.
2. Click the **Operation** tab and complete the following fields:

Configuration archive purge policy section	Choose the scope of the purge: • **Purge all archived configuration**—Choose to purge all files and configurations associated with selected device(s) or device group(s). • **Purge per policy**—Choose 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**.

Search the Archive for a Configuration

Use this task to search for a configuration in the configure archive for an existing configuration backup.

The following search criteria can be used:

- Standard wild card ***** and **?** characters are supported.
  - ***** matches 0 or more characters.
  - **?** matches 1 character.
- Search filters containing wild card characters must be enclosed in double quotes: **“fo*”**.
- Search filters containing no wild card characters result in an exact match.
- Wild card characters cannot be used outside of double quotation marks in combination with an exact match search.

  “A*1” is a valid search filter.

  “A*”* is not a valid search filter.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

1. Expand the **Configuration Manager** slider, and click to expand the **Configure archive** folder in the navigation pane.
2. Iin the navigation pane, click **Archive configuration**.
3. In the Archive configurations pane, click **Search**.
4. In the **Configuration archive search** dialog, complete any of the following fields:

Configuration name field	The user-defined name for the device configuration.
Source field	The source IP address of the device.

Hardware version field	The hardware version of a device.
Software version field	The software version of a device.
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. In the **Success** dialog, click **OK**.

   The newly-added physical interface appears in the **Physical interface** table.

Use Session Element Manager to Configure Product Devices

You can configure some basic parameters for product devices, which includes bootstrapping, system, SNMP, and traps, and the configuration of some basic networking parameters for session delivery products. See your session delivery product device documentation for more configuration information that is beyond the scope of this guide.

> **Note:**
>
> For Oracle Enterprise products, Session Element Manager supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Verify Product Device Configurations

The product device configurations you plan to manage using Oracle Communications Session Element Manager must have the correct system information configured to properly load into Configuration Manager. See the product device documentation for more information about the CLI commands that are used in these system configurations.

> **Note:**
>
> For Oracle Enterprise products, verifying the configuration supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Check Boot Parameters

Boot parameters specify the information that your Oracle Communications Session Delivery product device uses at boot time when it prepares to run applications. You must configure the system IP address, subnetwork (subnet) mask for the management interface (wancom0), and a unique target name.

> **Note:**
>
> Do not use the default session delivery product name **acmesystem**.

Oracle Communications Session Element Manager uses the target name to uniquely identify a device from the list of Oracle Communications Session Delivery product devices in the content area. You need to ensure that all Oracle Communications Session Delivery product devices you plan to load and manage have unique target names or the entire list of Oracle Communications Session Delivery product devices appear with the default acmesystem name.

> **Note:**
>
> For Oracle Enterprise products, check boot parameters supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Check the System Configuration Element

Ensure the **system-config** element, which establishes that general system information and settings for the product device is configured with the following SNMP and networking parameters:

- System contact information.
- System ID.
- Physical location of the system.
- SNMP is enabled on the system.
- Traps are enabled on the system.
- The network default gateway IP address is configured.

For more information about configuring these parameters, see your product device configuration documentation.

> **Note:**
>
> For Oracle Enterprise products, check system configuration supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Check the SNMP Community Element

The **snmp-community** element must be configured with the following parameters to specify the Oracle Communications Session Delivery Manager server from which your Oracle Communications Session Delivery product device accepts SNMP requests:

- Ensure that the Oracle Communications Session Delivery Manager server IP address is configured and the server is running.

- Ensure that the IP address(es) for SNMP communities are specified for authentication purposes. If the **snmp-community** element is configured for a cluster, you must add all the IP addresses for each member in the Oracle Communications Session Delivery Manager server cluster.
- If you change the snmp-community values for your Oracle Communications Session Delivery product device, you must remove this device from the Device Manager, and add it again so that the Oracle Communications Session Delivery Manager server can update this SNMP information.

> **Note:**
>
> For Oracle Enterprise products, check SNMP community supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Check the Trap Receiver Element

The **trap-receiver** element is configured on the Oracle Communications Session Delivery product devices so that the Oracle Communications Session Delivery Manager server can receive SNMP traps for event reporting. Ensure that the following parameters are specified:

- The Oracle Communications Session Delivery Manager server IP address is specified.
- The filter level must be set to **All**.
- The community name must match the name in the SNMP community element.

> **Note:**
>
> If you configure the trap-receiver element for a cluster, you need to add all the IP addresses for each member in an Oracle Communications Session Delivery Manager server cluster.

> **Note:**
>
> For Oracle Enterprise products, check trap receiver supports only the Enterprise Session Border Controller (ESBC) and the Enterprise Communications Broker (ECB).

Add Physical Interfaces

Use Oracle Communications Session Element Manager to add a physical interface for your session delivery device.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, select a device, and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, click **Add** in the **Physical interface** table.
6. In the **Add Physical interface** dialog, complete the following fields:

Name field	Enter a unique name for this interface using any combination of characters entered without spaces.
Operation type drop-down list	Select one of the following physical interface types: • **Maintenance**—The management physical interface that is used for management protocols or high availability (HA). • **Control**—This is a legacy parameter that can also be used to configure the management physical interface. • **Media**—The media interface, which carries production traffic.
Slot field	Enter the slot of this physical interface (**0** or **1**).
Port field	From left to right as you face the chassis, the possible values are from **0** to **3**.

7. Click **Apply**.
8. In the **Success** dialog, click **OK**.

   The newly-added physical interface appears in the **Physical interface** table.

Configure a Physical Interface

Use this task to configure a physical interface for a session delivery device.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.

4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, select a physical interface in the **Physical interface** table, and click **Edit**.
6. In the **Physical interface** pane, complete the following fields:

Auto-negotiation - 10/100Mbps field	If the default **enabled** is selected for the device, then this device and the device to which it is linked can automatically negotiate the duplex mode and speed for the link. If you want auto-negotiation disabled so that you can set these link parameters manually, select **disabled** to disable auto-negotiation and operate in **HALF** duplex mode (default) so that the devices do not engage in link negotiation or select **FULL** duplex mode to let both devices on a link send and receive packets simultaneously. You can set the connection speed to either **10** or **100** Mbps for **HALF** or **FULL** duplex mode.
Virtual MAC address field	Enter the virtual MAC address of the session delivery device.
Health score decrement for management interface failure% field	If you want to enter a value other than the default (**50** percent), enter the percentage that determines what is considered to be the active and standby health status of the physical interface for alarm purposes. This parameter is available if the **Maintenance** or **Control** parameter is selected for the **Operation type** field.

7. If you want to change the default alarm threshold for the physical interface (**minor**), click **Add** in the **Alarm threshold** section.
8. In the **Add Alarm threshold** dialog, select from the following **Severity** drop-down list filter levels for syslog and SNMP alarms:
   - **minor**
   - **critical**
   - **major**
9. Click **Apply**.
10. In the **Success** dialog, click **OK**.
11. Click **Apply** to finish configuring the physical interface.

Add a Network Interface

You must create a default network interface that is associated with your physical interface.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, select a device, and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, click **Add** in the **Network interface** table.

> **Note:**
>
> Click the arrow on the **Guidelines** box to view dependencies regarding your network interface.

6. In the **Add Network interface** dialog, complete the following fields:

VLAN number field	If this network interface is not channelized, keep this port set to 0 (default). If this network interface is channelized, enter the appropriate VLAN number (sub-port ID).
Physical interface drop-down list	Click the physical interface to which this network interface corresponds in the drop-down list.

7. Click **Apply**.
8. In the **Success** dialog, click **OK**.

   The newly-added network interface appears in the **Network interface** table.

Configure a Network Interface

Use this task to configure your session delivery device to communicate with any network element.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.
2. In the **Managed Devices** pane, select a device, and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Physical interface** table, click an existing physical interface.

   The network interface belonging to the selected physical interface appears in the **Network interface** table.
6. Select this network interface, and click **Edit**.

7. The **Interfaces** pane displays. In the **Host** section complete the following fields to configure network interface parameters for the device:

Host name field	The host name of this network interface. This field is populated with **default**.
IP address field	The IP address of this network interface.
Subnet mask field	The subnet mask of this network interface.
Primary IP Address field	The primary gateway that this network interface uses to communicate for the next hop route.
Secondary IP Address field	The secondary gateway of this network interface (if applicable).

8. To configure parameters that monitor the health of the gateway, click **Add** in the **Gateway heartbeat** section.
9. In the **Add Gateway heartbeat** dialog, complete the following fields:

State drop-down list	Select to **enable** or **disable** the gateway heartbeat feature. The default value is **enabled**.
Expected ARP message interval from gateway (sec) field	The number of seconds between heartbeats for the media interface gateway. Heartbeats are sent at this interval as long as the media interface is viable. The default value is **0**. The valid range is from **1** to **65535**. The value you configure in this field overrides any globally applicable value set in the gateway heartbeat interval parameter in the device HA node (redundancy) configuration.
Number of ARP request retransmissions (#) field	The number of heartbeat retries that you want sent to the media interface gateway before it is considered unreachable. The default value is **0**. The valid range is from **1** to **65535**.
ARP request timeout (sec) field	The heartbeat retry time-out value in seconds. The default value is **1**. The valid range is from **1** to **65535**. This parameter sets the amount of time between device ARP requests to establish media interface gateway communication after a media interface gateway failure.
Health score decrement-gateway or link failure field	The amount to subtract from the device health score if a media interface gateway heartbeat fails. If the value you set in the retry-time-out field is exceeded, this amount is subtracted from the overall health score of the system. The default value is **0**. The valid range is from **0** to **100**.

10. Click **Apply**.
11. To configure tunnel parameters for the device, click **Add** in the **Tunnel config** section.
12. In the **Add Tunnel config** dialog, complete the following fields:

Name field	The unique name for the IPsec tunnel configuration.
Local IP address field	The local public IP address that terminates the IPSec tunnel.
Remote IP address field	The remote public IP address that terminates the IPSec tunnel.

13. Click **Apply**.
14. In the **DNS** section, complete the following fields to set a specific IP address for the network interface and others that are related to different types of management traffic:

Primary field	The domain name server (DNS) server for this network interface.
First backup field	The secondary DNS server for this network interface (if applicable).
Second backup field	The third DNS server for this network interface (if applicable).
Default domain name	The default domain for use with DNS queries.
DNS timeout	The DNS timeout value.

15. To configure (HIP) host-in-path firewall functions that are used to open well-known ports for services such as FTP, ICMP, SNMP, and Telnet over the media interfaces, complete the following fields:

HIP IP addresses box	The IPv4 addresses of the front panel network interfaces that are allowed to pass administrative traffic to the host. Adding HIP entries automatically opens the well-known port associated with a service.
FTP address field	The FTP interface IP address.
ICMP addresses box	The ICMP interface IP address(es).
SNMP address field	The SNMP interface IP address.
Telnet address field	The Telnet interface IP address.
SSH address field	The SSH interface IP address.

16. Click **Apply**.
17. In the **Success** dialog, click **OK**.

Save and Activate Device Configurations

During the save and activation process, other users cannot make changes to the device.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and click **Devices**.

2. In the **Managed Devices** pane, select a device, and click **Load**.
3. In the **Managed Devices** panel, click the **Home** folder to expand the configuration navigation tree for the loaded device.
4. Select the device, and click **Update**.
5. In the **Update configuration** dialog, click one of the following update operations:
   - **Save & activate configuration**—(Default) Invokes the save and activate process
   - **Save configuration**—Invokes the save process.
   - **Activate configuration**—Makes this configuration the running configuration on the device.
6. Click **OK**.
7. In the **Information** dialog, click **OK**.

   The operation you selected appears in the **Device tasks** table.
8. In the **Device tasks** table you can the operation row and click **View log** to get logging data for your device or save logging data to file on your local system.

4

Configure and Apply Global Parameters to Devices

You can target specific configuration changes to the parameters in Configuration Manager. You can then use a global parameter work order to apply these changes across a group of targeted devices that must have the same software version and hardware platform.

In any configuration, there are parameters that can apply equally to all targeted devices, and parameters such as hostnames, IP addresses, and so on that are unique to each device. To apply a configuration to multiple targeted devices and still be able to do the type of individual parameter changes that are required for individual devices, you must configure global parameters in the configuration. You can either add global parameters to an existing configuration schema (supported by OCSEM) that has empty configuration elements, or manually upload a configuration schema file from a device that is populated with parameters.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

After you are finished the tasks in this chapter, see the View Work Order Information chapter to view information for the work order(s) you configured.

Verify Your User Permissions to Apply Global Parameters

The ability to configure and apply global parameters on targeted devices depends on the user permissions that you were assigned in Security Manager and product plugin service features. You can do certain operations when you are logged in as one of the following user types:

- **LIAdministrators** and **administrators**—You can create, modify, execute, delete and control a work order.
- **dministrators**—You can create, modify, execute, delete and control a work order.
- **provisioners**—You can execute and control (start, abort, pause, resume, or commit) a work order.
- **monitors**—You can view work orders only.

> **Note:**
>
> Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.

> **Note:**
>
> The Oracle Enterprise Session Border Controller does not support **LIAdministrators**.

See the *Configure Security Privileges for Session Delivery Products* section in the *Security* chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.

Add a Global Parameter Configuration for Global Parameters

You can either add a global parameter configuration schema from a device or from an existing software schema in Oracle Communications Session Element Manager for configuring global parameters.

Add a Global Parameter Configuration from a Managed Device

> **Note:**
>
> A global parameter configuration stores the configuration changes to be applied in your global parameter work order.

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. In the **GP Config** tab, click **Add**.
3. In the **Add global configuration** pane, complete the following fields:

> **Note:**
>
> The **Category** field, and **Component**, **Platform**, and **Supported software version** drop-down lists are not available when the **Managed device** selection is made.

Configuration name field	The unique global parameter configuration name that is an alphanumeric value from 1 to 24 characters with no spaces and no special characters with the exception of the hyphen (-) and underscore (_).

	Note: When you choose a name for a new global parameter configuration, this name must not start with the prefix "ID". A validation error (invalid oc name) occurs if the above rules are not followed.
Description field	The description of the global parameter configuration.
Global configuration seeded from drop-down list	Select **Software version** to load the global parameter configuration from a managed device.
Selected Managed device field	Select the ellipsis icon (**...**) to choose the managed device that you want to use as a template for your global parameter configuration. The configuration data model from the selected device is loaded to the global parameter configuration, which contains the elements that are required for this device model and its unique device configuration values. In the **Select managed device** dialog box, select a device and click **OK**.

4. Click **Apply**. The following actions are taken:

   The global parameter configuration appears in the **GP Config** table.

Add a Global Parameter Configuration from a Software Version

A global parameter configuration stores the configuration changes to be applied in your global parameter work order. You can add a global parameter configuration from an existing software (schema) version.

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. In the **GP Config** tab, click **Add**.
3. In the **Add global configuration** pane, complete the following fields:

Note:

The **Selected Managed device** field is not available when the **Software version** selection is made.

Configuration name field	The unique global parameter configuration name that is an alphanumeric value from 1 to 24 characters with no spaces and no special characters with the exception of the hyphen (-) and underscore (_).

	Note: When you choose a name for a new global parameter configuration, this name must not start with the prefix "ID". A validation error (invalid oc name) occurs if the above rules are not followed.
Description field	The description of the global parameter configuration.
Global configuration seeded from drop-down list	Select **Software version** to load the existing software schema provided by the product plugin. The data schema for a selected device software version model and default values are loaded to the global parameter configuration. If you select this option, you must select a platform and software version. The available platforms and software versions are determined by the configuration schemas supported by the product plugin.
Category	Select the ellipsis icon (**...**). In the **Select Category** dialog box, select the product category and click **OK**. For example, for the Service Provider (SP) Edge and Core element manager product category you would select **SP Edge &Core**.
Component drop-down list	The available network function (NF) components are driven by the selection of the product category (default).
Platform drop-down list	Select the device hardware platform of the targeted devices.
Supported software version drop-down list	Select the software version of the device you want to use for your global parameter configuration.

4. Click **Apply**. The following actions are taken:

   The global parameter configuration appears in the **GP Config** table.

Manage the Global Parameter Configuration

Edit Information for a Global Parameter Configuration

1. Expand the **Configuration Manager** slider and click **Configuration tools**, **Global Parameters**.
2. In the **GP Config** tab, select the global parameter configuration you want to edit from the table and click **Edit**.
3. In the **Edit global parameter configuration** dialog box, enter the description that you want for this global parameter configuration. If you are logged into Oracle Communications Session Delivery Manager as the Lawful Intercept (LI) administrator user, you can enter the LI encryption password for the LI

configuration. Note that the LI encryption password parameter is not available for the Enterprise Edge and Core plug-in at this time.

> **Note:**
>
> You cannot edit the global parameter configuration name.

4. Click **OK**.

> **Note:**
>
> Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.

Edit the Global Parameter Configuration

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. In the **GP Config** tab, select the global parameter configuration you want to edit from the table and click **Load**.
3. In the success dialog box, click **OK**.

   The global parameter configuration name now appears below the **Global Parameters** icon as an expanded folder in the slider.
4. Expand configuration folders in the **Configuration Manager** slider to access configuration elements and sub-elements of the global parameter configuration.
5. Make changes to the global parameter configuration as you would a single device. See your product device documentation for specific configuration instructions.

> **Note:**
>
> Each time you apply configuration changes in your global parameter configuration, the modifications are added to the database. They are not provisioned to your device until you execute and commit your global parameter work order. The LCV logs additions, deletions, and modifications of top-level elements.

View Global Parameter Configuration Changes

View global parameter configuration changes to track any modifications that are made to the global parameter configuration schema in the Local Configuration View (LCV) that lists the element types that are added, deleted or modified.

1. Expand the **Configuration Manager** slider and click the **Global parameters**.
2. In the **GP Config** tab, select the global parameter configuration and click **View Changes**.
3. The **Local configuration view** table appears in the content area and displays the top-level element changes for this global parameter configuration.

4. You can select a top-level element and click **View Detail** for further attribute modification details.

Configure a Global Parameter Work Order

Use the tasks in this section to configure a global parameter work order that is used to apply configuration parameter changes across a group of up to 20 targeted devices.

> **Note:**
>
> The parameters in the global parameter configuration are validated across multiple devices simultaneously. For success, a global parameter work order must be used across devices with the same software version and platform.

Add a Global Parameter Work Order

1. Expand the **Configuration Manager** slider and click **Configuration tools** and select **Global Parameters**.
2. Click the **Admin** tab and click **Add** in the **Work orders** table.
3. In the **Settings** tab, configure the following parameters:

Name	The work order name, which is an alphanumeric value from 1 to 24 characters in length with no spaces.
Scheduled check box	Check the check box to enable the **Start date and time** field to schedule when the global parameter work order starts.
Start date and time field	Select a start date 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.
Run device tasks concurrently check box	Check the check box to run global parameter work order tasks at the same time multiple device group tasks are updated concurrently. If you select this check box the **Error policy** and **Behavior** fields cannot be configured.
Error policy drop-down list	Error policies that determine how errors are handled when they occur during the execution of your global parameter work order. Select from the following error policies you want to apply to this global parameter work order: • **Log and proceed**—(Default) The targeted device that experiences the error is rolled back to its original configuration state and the work order proceeds to the next targeted device in the work order list. • **Stop**—The targeted device that experienced the error is rolled back to its original configuration state and the work order stops. You must manually resume, or abort, the work order.

	• **Stop and rollback**—All targeted devices are stopped until the error is rolled back, devices are returned to their original configuration state, and the work order stops.
Behavior drop-down list	This drop-down list is disabled by default which means that this parameter is set to **Automatic**. Select from the following behaviors to apply to this work order: • **Automatic** (default)—The software upgrade or global parameter changes proceeds on each targeted device without requiring intervention. • **Device-level**—The software upgrade or global parameter changes pause after each targeted device finishes updating. You must manually continue to the next targeted device listed in the work order. **Note:** If an error occurs during the work order execution, the behavior is controlled by the error policy.
Auto commit check box	When a work order 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 work order is successfully committed and its devices are unlocked. The check box is disabled by default, which means the work order must be manually committed from the work order. Check the check box to automatically commit the global parameter work order after the execution of the work order.

4. Select the **Device groups** tab and click **Add** in the **Device groups** table.
5. In the **Select Device** dialog box, expand a device folder in the **Managed devices** table, select a device row, and click **Add**.
6. 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:

- A work order is limited to one platform and software version at a time.
- In the case of a high-availability (HA) device pair, the work order is applied to both devices.
- All devices must have the same platform, software version, and same redundancy type (HA or standalone).

7. Repeat the previous steps to add additional targeted devices.

> **Note:**
>
> Device filtering is applied after the first device is selected.

8. Click **OK**. The devices appear in the **Device groups** and **Devices** tables.
9. Click the **Global parameter changes** tab.
10. Click the ellipsis (**...**) icon next to the **Global configuration** field to select your global parameter configuration.

> **Note:**
>
> A global parameter configuration must have the same software version and platform as the selected devices.

11. In the **Select global configuration** dialog box, select the global parameter configuration you want to assign to this global parameter work order and click **OK**.

    The **Global configuration** field populates with the global parameter configuration you selected and the **Version number** field displays its software version.
12. Click **Apply**.
13. In the success dialog box, click **OK**.

    The global parameter work order appears in **Work orders** table.

Load a Global Parameter Configuration

Load a global parameter configuration for storing global parameter changes.

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. In the **GP Config** tab, select a global parameter configuration from the table and click **Load**.

   Once the global parameter configuration loads, the global parameter configuration name appears below the **Global parameters** icon. Any configurations made under this folder are contained in the global parameter configuration, and applied to targeted devices through a work order.

> **Note:**
>
> The global parameter configuration name also appears at the top of the content area when it is loaded.

Configure the Global Parameter Work Order Element Criteria

Use this task to specify a criteria for one or more element attributes to which you want to apply changes on your targeted devices before you execute the global parameter

work order. If there is only one attribute for a system-wide element, no criteria needs to be specified for the global parameter work order.

> **Note:**
>
> An element attribute is dynamic and changes depending on its type for which you are setting a criteria. Some elements may require that a criteria is specified for certain element attributes before the global parameter work order is executed.

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. Click the **Admin** tab and select the global parameter work order, which contains the global parameter configuration for which you specify the criteria, from the **Work orders** table.
3. Click **Edit**.
4. Click the **Global parameters changes** tab and select the element name for which you want to specify criteria and click **Set criteria**.
5. In the **Set criteria** dialog box, click **Add**.
6. In the **Add criteria** dialog box, enter the CLI attribute name.

   > **Note:**
   >
   > The **Add criteria** dialog box automatically prompts you for the exact attributes that make up the primary key for the selected type of configuration element attribute. The element attribute is specified by using whatever “key” attribute values are appropriate for its type. For example, the key for a session agent is **hostname**.

7. Enter the specific criteria needed.

   > **Note:**
   >
   > You must know which values are considered valid for the particular attribute for which you are setting a criteria.

8. Click **OK**. The criteria is added to the **Criteria** column in the **Configuration** table.
9. Check the **Apply change to all instances** check box to apply the criteria that you add to all element attributes of this multiple element.
10. Click **OK**.
11. Repeat the previous steps if you want to set multiple criteria element attributes.
12. Click **Apply**.
13. In the success dialog box, click **OK**.

Execute a Global Parameter Work Order Manually

Once the software upgrade work order is created and its configuration is applied, it can be executed manually (unless you previously scheduled a start date and time for it to execute).

1. Expand the **Configuration Manager** slider and click **Global parameters**.
2. Click the **Admin** tab.
3. In the **Work orders** table, select the work order you want to execute and click **Start**.
4. In the confirmation dialog box, click **Yes**.
5. Click **Refresh** to confirm the status changes for your global parameter work order from **Not Scheduled** to **Running**.

Commit a Global Parameter Work Order Manually

After a global parameter work order is executed, it must be committed to unlock the targeted devices that are associated with the global parameter work order. A global parameter work order is committed manually if the **Auto commit** check box is unchecked in the global parameter work order.

Only global parameter work orders with a status of **Success**, **Failed**, **Aborted**, **AbortFailed**, or **CommitFailed** can be committed. When you commit a global parameter work order, all targeted devices associated with this work order are unlocked and this global parameter work order can no longer be modified or rolled back. You must create a new global parameter work order to implement new changes. Until the global parameter work order is committed, you can stop it and perform a rollback to restore the original software version or original configuration settings.

1. Expand the **Configuration Manager** slider and click the **Admin** tab.
2. In the **Work orders** table, select the work order you want to commit and click **Commit**. A confirmation dialog box appears.
3. In the confirmation dialog box, click **Yes**.
4. Click **Refresh** to confirm the work order status changed from **Success** to **Committed**.

Manage Global Parameter Work Orders

Preview Global Parameter Work Order Device Configuration Changes

You can view a summary of the necessary changes (preview) for the targeted device(s). For example, if a third-level sub-element is added to a global parameter configuration, it is possible that one of the targeted devices did not contain the higher-level elements in their current saved configuration. Those top-level instances are added by the Oracle Communications Session Element Manager, and the preview shows the required updates for these targeted devices. The preview output is different for every targeted device in a global parameter work order based on its original configuration.

1. Expand the **Configuration Manager** slider and click **Global parameters**.

2. Click the **Admin** tab and select a global parameter work order from the **Work orders** table.
3. In the **Device tasks** table, select a device task for your global parameter work order and click **Preview**.

   A preview of the required updates for the targeted device appear in the content area.

Delete a Global Parameter Configuration

1. Expand the **Configuration Manager** slider and click the **Global parameters**.
2. In the **GP Config** tab, select the global parameter configuration that you want to delete and click **Delete**.
3. In the **Delete** confirmation dialog box, click **OK**.

5

Configure and Apply Software and Bootloader Upgrades to Devices

You can use software and bootloader upgrade work orders to apply automatic upgrades across a group of targeted devices that have the same software version and hardware platform in Device Manager.

After you are finished the tasks in this chapter, see the "View Work Order Information" chapter to view information for the work order(s) you configured.

Verify Your User Permissions to Apply Software and Bootloader Upgrades to Devices

The ability to apply software and bootloader upgrades on targeted devices depends on the user permissions that you were assigned in Security Manager and product plugin service features. You can do certain operations when you are logged in as one of the following user types:

- **LIAdministrators** and **administrators**—You can create, modify, execute, delete and control a work order.
- **provisioners**—You can execute and control (start, abort, pause, resume, or commit) a work order.
- **monitors**—You can view work orders only.

> **Note:**
>
> Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.

> **Note:**
>
> The Oracle Enterprise Session Border Controller does not support **LIAdministrators**.

See the *Configure Security Privileges for Session Delivery Products* section in the *Security* chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.

Add a Software Image to the Software Image Archive Directory

The software image archive allows you to view, load and delete all device software images maintained by the Oracle Communications Session Element Manager.

Before you create your software upgrade work order, you must upload the correct software image to the software image archive on the server directory.

If the Oracle Communications Session Delivery Manager server on which Oracle Communications Session Element Manager is in a cluster, this server ensures that the new image is replicated for all nodes in the cluster.

1. Expand the **Device Manager** slider and select **Software upgrade**, **Software image archive**.
2. Click **Add**.
3. In the **Upload software to image to archive dialog** box, select the plug-in category from the **Categories** table (for example, SP Edge & Core) and click **Browse** from the **File** field.
4. In the **File Upload** dialog box that displays, navigate the directory structure on your system to the new software image, select it, and click **Open**.
5. The file you uploaded appears in the **File** field. Click **Upload**. The software image file appears in the **Software Image Archive** table, which contains the following fields:

Device software image archive home	The directory to which the software image files are uploaded.
Device software image name	The device software image name.
Size (Bytes)	The software image file size in bytes.
Date	The date and time when the file was stored to the disk.

Add a Bootloader Image to the Bootloader Image Archive Directory

The bootloader image archive allows you to view, load, and delete all device bootloader images maintained by the Oracle Communications Session Element Manager.
Before you create your bootloader upgrade work order, you must upload the correct bootloader image to the bootloader image archive on the server directory:

```
AcmePacket/NNCArchive/BootImageArchive/<vendor-key>-<product-key>/
<plugin-name-key>
```

Based on your Network Function (NF) type, the image is then uploaded into one of the following sub-directories:

- Oracle-SessionDelivery/AcmeSD
- Oracle-enterprise/Enterprise
- Oracle-enterpriseext/EnterpriseExt

If the Oracle Communications Session Delivery Manager server on which Oracle Communications Session Element Manager is in a cluster, this server ensures that the new image is replicated for all nodes in the cluster.

1. Expand the **Device Manager** slider and select **Software upgrade**, **Boot Loader image archive**.
2. Click **Add**.
3. In the **Upload Bootloader image to archive** dialog box, select the plug-in category from the **Categories** table (for example, SP Edge & Core) and click **Browse** from the **File** field.
4. The file you uploaded appears in the **File** field. Click **Upload**. The bootloader image file appears in the Bootloader Image Archive table, which contains the following fields:

Boot Loader image file name	The name of the uploaded bootloader image file.
Size (Bytes)	The bootloader image file size in bytes.
Date/Time created	The date and time when the file was stored to the disk.
Archive path	The directory to which the archive image files are uploaded.

Add an Upgrade Work Order

1. Expand the **Device Manager** slider and select **Software upgrade**, **Work order administration**.
2. In the **Work orders** table, click **Add**.
3. In the **Settings** tab, configure the following parameters:

Name	The work order name, which is an alphanumeric value from 1 to 24 characters in length with no spaces.
Scheduled check box	Check the check box to enable the **Start date and time** field to schedule when the upgrade work order starts.
Start date and time field	Select a start date 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.
Run device tasks concurrently check box	Check the check box to run the upgrade work order device tasks at the same time. If you select this check box the **Error policy** and **Behavior** fields cannot be configured.

Error policy drop-down list	Error policies that determine how errors are handled when they occur during the execution of your upgrade work order. Select from the following error policies you want to apply to this upgrade work order: • **Log and proceed**—(Default) The targeted device that experiences the error is rolled back to its original configuration state and the work order proceeds to the next targeted device in the work order list. • **Stop**—The targeted device that experienced the error are rolled back to its original configuration state and the work order will stop. You must manually resume, or abort, the work order. • **Stop and rollback**—All targeted devices are processed until the error is rolled back, devices are returned to their original configuration state, and the upgrade work order stops.
Behavior drop-down list	Select from the following behaviors that apply to this upgrade work order: • **Never pause**—(Default) The upgrade proceeds on each targeted device without requiring intervention. • **Pause after every device**—The upgrade pauses after each targeted device finishes updating. You must manually continue to the next targeted device listed in the work order. **Note:** If an error occurs during the work order execution, the behavior is controlled by the error policy. • **Pause after the first device**—The upgrade work order changes pause after the first targeted device finishes updating. You must manually continue the operation. After that, the next targeted devices listed in the work order proceed without requiring intervention. **Note:** If an error occurs during the work order execution, the behavior is controlled by the error policy.
Device operation timeout (minutes)	The timeout in minutes after which the upgrade work order operation ceases on a device.
Auto commit check box	When an upgrade work order 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 work order is successfully committed and its devices are unlocked.

	The check box is disabled by default, which means the work order must be manually committed from the work order. Check the check box to automatically commit the global work order after the execution of the upgrade work order.

4. Click the **Device groups** tab and click **Add**.
5. In the **Select Device** dialog box, expand a device folder in the **Managed devices** table, select a device row, and click **Add** to move the device to the **Targeted devices** table.
6. 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:
>
> - A work order is limited to one platform and software and bootloader version at a time.
> - In the case of an high-availability (HA) device pair, the work order is applied to both devices.
> - All devices must have the same platform, software version, bootloader version, and same redundancy type (HA or standalone).
>
> to one Work orders are moved to the targeted devices.

7. Repeat the previous steps to add additional targeted devices.
8. Click **OK**.

   The devices appear in the devices table.
   The devices table shows the IP address or FQDN depending on the details added by the user in the Device Manager.
9. Click the **Workflows** tab, and complete the following required and optional fields:

Targeted software image field	Click the ellipse (**...**) icon to select the targeted software image that you are upgrading from the **Select node software image** dialog box and click **OK**.
Boot Loader Upgrade field	(Optional) Check the check box to include a Bootloader image upgrade.
Targeted boot image field	When Boot Loader Upgrade is checked, click the ellipse (**...**) icon to select the targeted bootloader image that you are upgrading from the **Select node bootloader image** dialog box and click **OK**.

	Note: Once you click **OK**, the OCSEM performs a compatibility check between the "Targeted software image" and the "Targeted Bootloader image" files and if a failure occurs, the following message displays: `Targeted software image version and Bootloader image version are different, do you still want to proceed...` .
Health score threshold (%) field	(Optional) The high availability (HA) health score percentage from 1 to 100 percent that is applicable to HA pairs only. During the upgrade process, Oracle Communications Session Element Manager checks the health score to determine if the devices are in a stable condition. If the health score value is set, and the device health is not above the health score value, the upgrade does not proceed.
Restore original redundancy states after upgrade check box	(Optional) Check the check box to restore the original HA setup after the upgrade is complete.
Reject new call check box	(Optional) Check the check box to enable call shedding on a standalone device. The device re-boots when the active-call threshold reaches its limit during the upgrade process. See the device performance management MIB to view the current call-shedding count. The default is **disabled**.
Active call threshold field	(Optional) The threshold number of active calls below which the upgrade or downgrade reboot proceeds automatically.
Pause and unlock after loading image check box	(Optional) Check the check box to intentionally pause the upgrade work order after the image is delivered to all targeted devices. Targeted devices are unlocked once the image is successfully delivered.
Remove old image from device on commit	(Optional) Check the check box to remove the old device image on the devices after the execution and commit of the work order.

10. Select the **Pause after** checkbox next to any work flow step of the processing of the upgrade work order to pause it. When a break point is inserted, the work order is stopped after the step before the work flow step completes successfully. You must manually resume the work order so that the devices can re-boot with the new upgrade images.

    The following **Work flow** table columns are described below:

    - **Step**—The number of this task in the work flow order.

- **Description**—The description of the task associated with this step.
- **Pause after**— When checked, enables a break point after this step has successfully completed. The default is **disabled**.

11. Click **Apply**. The upgrade work order appears in the **Work orders** table.

Execute Upgrade Work Orders Manually

Once the upgrade work order is created and its configuration is applied, it can be executed manually (unless you previously scheduled a start date and time for it to execute).

1. Expand the **Device Manager** slider and select **Software upgrade**, **Work order administration**.
2. In the **Work orders** table, select the work order you want to execute and click **Start**.
3. In the confirmation dialog box, click **Yes**.
4. Click **Refresh** to confirm the status changes for your upgrade work order from **Not Scheduled** to **Running**.

Commit Upgrade Work Orders Manually

After an upgrade work order is executed, it must be committed to unlock the targeted devices that are associated with the upgrade work order. An upgrade work order is committed manually if the **Auto commit** check box is unchecked in the upgrade work order.

Only upgrade work orders with a status of **Success**, **Failed**, **Aborted**, **AbortFailed**, or **CommitFailed** can be committed. When you commit an upgrade work order, a rollback is no longer possible, all targeted devices associated with this work order are unlocked, and this upgrade work order can no longer be modified. You must create a new upgrade work order to implement new changes. Until the upgrade work order is committed, you can stop it and perform a rollback to restore the original software or bootloader version or original configuration settings.

1. Expand the **Device Manager** slider and click **Software upgrade** and then **Work order administration**.
2. In the **Work orders** table, select the work order you want to commit and click **Commit**. A confirmation dialog box appears.
3. In the confirmation dialog box, click **Yes**.
4. Click **Refresh** to confirm the work order status changed from **Success** to **Committed**.

Manage Upgrade Work Orders

Delete a Software Image from the Software Image Archive Directory

1. Expand the **Device Manager** slider and select **Software upgrade**, **Software image archive**.
2. Select the software image file you want to delete from the archive home directory and click **Delete**.
3. In the success dialog box, click **OK**.

   The software image file is removed from the **Software Image Archive** table.

Delete a Bootloader Image From the Bootloader Image Archive Directory

1. Expand the **Device Manager** slider and select **Software upgrade**, **Boot Loader image archive**.
2. Select the bootloader image file you want to delete from the archive directory and click **Delete**.
3. In the success dialog box, click **OK**.

   The bootloader image file is removed from the **Bootloader Image archive** table.

Configure Downgrade Work Orders

Use the same tasks in the "Add Upgrade Work Orders" section if you need to do a downgrade across a group of targeted devices. The only difference is you must add a previous version of the software or bootloader image to the software image archive directory and bootloader image directory and select this software image later when you add the downgrade work order. The limitation is that some device downgrades may not supported. See your device product documentation for more information.

Refresh the Bootloader Image Archive List

1. Expand the **Device Manager** slider and select **Software upgrade**, **Boot Loader image archive**.
2. Click **Refresh**.

   The Bootloader Image Archive list is updated from the BootImageArchive directory.

Work Flow Processing Scenarios for an Upgrade Work Order

An upgrade work order contains a predefined work flow that lists the execution procedure sequentially in a step-by-step process. As the upgrade work order is executed, each procedural step is tracked in the **Device tasks** table, under the **Progress** column. The following sections outline the different upgrade work-order scenarios:

Upgrade for a Standalone Device

1. The available space is checked for the device.
2. The current device software and/or bootloader image is archived.
3. The running configuration data file is retrieved for backup.
4. The software and/or bootloader image is pushed to the device.
5. Call shedding is performed.
6. The configuration file is converted to ACP XML format if necessary.

7. The image name in the boot parameters for the device is edited.
8. The device is re-booted.
9. The Oracle Communications Session Element Manager plugin updates the device information in the Oracle Communications Session Delivery Manager server.

Upgrade for a High Availability Device Pair

1. The available space is checked for both devices.
2. The status and health is checked for both devices.
3. The current device software and/or bootloader image is archived.
4. The running configuration data file is retrieved for backup.
5. The software and/or bootloader image is pushed to both devices.
6. The configuration file is converted to ACP XML format if necessary.
7. The image name in the boot parameters for the standby device is edited.
8. The standby device is re-booted.
9. The health of the standby device is checked.
10. A fail-over is forced and the standby device becomes the active device.
11. The image name in the boot parameters for the new standby device is edited.
12. The new standby device is re-booted.
13. The Oracle Communications Session Element Manager plugin updates the device information in the Oracle Communications Session Delivery Manager server.

Rollback for a Standalone Device

> **Note:**
>
> The rollback steps below are for a successfully-executed device task and may vary if the rollback process is initiated when a work order fails or is aborted during the execution process.

1. The files are pushed to the standalone device.
2. Call shedding is performed.
3. The image name in the boot parameters is edited.
4. The device is re-booted.
5. The device information in Oracle Communications Session Delivery Manager is updated.

Rollback for an HA Pair

> **Note:**
>
> The rollback steps below are for a successfully-executed device task and may vary if the rollback process is initiated when a work order fails or is aborted during the execution process.

1. Files are pushed to both devices.
2. The status and health score are retrieved from both devices.
3. The image name in the boot parameters from the standby device is edited.
4. The standby device re-boots.
5. There is a switch-over to a standby device.
6. The image name in the boot parameters is edited from the standby device.
7. The new standby device is re-booted.
8. The device information in Oracle Communications Session Delivery Manager is updated.

6

View Work Order Information

Use the tasks in this chapter to view work order information in Dashboard Manager, Device Manager, and Configuration Manager.

View Work Orders

1. Use one of the following actions to access work order information:
   - All work order types—**Dashboard Manager**, **Work order view**, **Work order administration**.
   - Software upgrade work order—**Device Manager**, **Software upgrade**, **Work order administration**.
   - Global parameter work order—**Configuration Manager**, **Global Parameters**, and click the **Admin** tab.
2. In the **Work orders** table, the following column information is displayed:

Name	The work order name.
Device count	The number of targeted device nodes (standalone devices or HA pairs) the work order executes. An HA pair is considered one device node.
Configuration Name	(Global parameter work order only) The global parameter configuration name is applied in this global parameter work order.
Target SW version	(Software upgrade work order only) The software version to be installed.
Status	A work order can have the following status: • **PartiallyConfigured**—The configuration is incomplete. • **NotScheduled**—The start time is not yet configured. • **Scheduled**—The start time is configured and scheduled to begin at a specified date and time. • **WaitStarting**—The work order is placed into a run-waiting queue by the server's scheduler and awaits the scheduled time to start running. • **Running**—The work order started and is currently processing. • **Pausing**—The work order pauses after **Pause** is initiated by the user. Pausing is useful for testing purposes to check and validate changes on a targeted device. • **Paused**—The work order stopped completely. You must manually resume a stopped task or abort the task. • **Resuming**—The work order resumes processing.

	• **Success**—The work order completed successfully, but has not yet been committed. • **Failed**—The work order failed during execution. • **StartCommitting**—The work order started the process of committing the designated changes. • **Committing**—The work order is in the process of committing the designated changes. • **Committed**—The changes were executed successfully by this work order and are now committed. • **CommitFailed**—The work order failed to commit and some of the locked resources or the auto-generated files may fail to remove. • **StartAborting**—The work order is in the beginning process of aborting. • **Aborting**—The work order is executing the abort process. • **Aborted**—The work order 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 work order failed to abort due to a failure of a device rollback process. • **Preloading**—This status applies to software upgrades only. The state the work order is in when the Pause and unlock after loading software image parameter is enabled in the software upgrade configuration, and the work order is loading the target software image to all targeted devices. • **PreloadPause**—This status applies to software upgrades only. This state occurs after the work order successfully delivered the target software image to the targeted devices and unlocked the devices. You can resume the work order in this state. • **PreloadFailed**—The work order failed to load the target software image to all targeted devices. • **LockingResource**—The state when the work order locks all necessary resources. • **LockResourceFailed**—The work order 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 this work order.
End time	The end time is the server local time when the following conditions occur for this work order: • 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 Tasks

1. Use one of the following actions to access device task information that is associated with one of the following work order types:
   - All work order types—**Dashboard Manager**, **Work order view**, **Work order administration**.
   - Software upgrade work order—**Device Manager**, **Software upgrade**, **Work order administration**.
   - Global work order—**Configuration Manager**, **Global Parameters**, and click the **Admin** tab.
2. In the **Device Group tasks** table, the following column information is displayed:

Device group	The device group name.
Network function	The name of the network function (NF) to which the device(s) belong.
Platform	The platform of the devices.
SW version	The software version of devices.
Status	A device task can have the following status: • **Ready**—The task is ready to run and waiting for the Oracle Communications Session Element Manager plugin to schedule it to start. • **ResetToReady**— When the work order restarts, all the failed tasks are reset to this state to distinguish the initial **Ready** state of the task. • **Starting**—The intermediate state between the **Ready** and **Running** states when users submit or resubmit the task. • **Running**—The task started and is currently processing. • **Pausing**— The intermediate state between **Running** and **Paused** states when you click **Pause**. • **Paused**—The task stopped completely, which is initiated by setting an error policy to halt. You must manually resume a stopped task or abort the task. • **Success**—The task completed successfully. • **Failed**—The task failed during execution and any changes are rolled back. • **StartRollingBack**—The task starts to abort when you click **Abort**. • **RollingBack**—The task is executing the rollback procedure when either when you click **Abort** or the device task normally and automatically rollbacks due to an error during the normal execution of the device task procedures. • **RolledBack**— The task is rolled back successfully.

	• **RollBackFailed**—The task is rolled back unsuccessfully. • **Preloading**—The task is loading the target software image to the device. • **PreloadPause**— The task loaded the target software image and paused. • **PreloadFailed**—The task failed to load the target software image to the targeted device(s).
Progress	The number of the steps out of the total number of steps that must be executed for the process to complete successfully.
Start time	The server start date and local time at which the work order was scheduled to start or the time when a task within a work order is started. The following criteria are used: • If the work order has not reached its scheduled start time for all individual tasks for this work order to display the same start time. • When an individual task starts, it replaces the scheduled start time with the time it started processing.
End time	The end time is the server local time when the following conditions occur for this device task: • The device task finished successfully and paused. • A failed condition has been met and the device task stopped as a result of the failure. • The user manually stops a device task already in progress.

View Work Order and Device Group Task Logs

1. Use one of the following actions to access work order or device task information:
   - Global parameter work order—**Configuration Manager**, **Global Parameters**, and click the **Admin** tab.
   - Software upgrade work order—**Device Manager**, **Software upgrade**, **Work order administration**.
   - All work order types—**Dashboard Manager**, **Work order view**, **Work order administration**.
2. In the **Work orders** table for a global parameter work order that is running or executed, click **Logs** to view the following logging information:
   - Pause, start or resume, abort or rollback, and commit actions.
   - Pause, resume, abort or rollback, and resubmit task actions.
3. In the **Work orders** table for a software upgrade work order that is running or executed, click **Logs** to view the following logging information:
   - Software archive and software upgrade actions.
   - Pause, start or resume, abort or rollback, and commit actions.
   - Pause, resume, abort or rollback, and resubmit task actions.

4. In the **Device group tasks** table for device tasks that are associated with a global parameter work order or software upgrade work order that is running or executed, click **Logs** to view the following logging information
   - Global parameter configuration changes, including addition, modification, and deletion of parameters.

Work Order Processing States and User Actions

The following sections chart the various actions you can or cannot perform during internal processing state of your global or software upgrade work order. The internal processing state is associated with the predefined process flow for each work order type. The actions in the **Work orders** table and the **Device group tasks** table are dynamically enabled or disabled based on the state of the selected work order, or on a device group task within the work order. A warning dialog box appears if you attempt an action that is not allowed during a certain state.

Work Order States and When to Perform Actions

The following matrix describes the different work order processing states and when you can perform actions on them.

States Below:	Action: Edit	Action: Delete	Action: Copy	Action: Commit	Action: Abort	Action: Start	Action: Restart	Action: Resume	Action: Pause
Partially-Configured	Yes	Yes	Yes	No	No	No	No	No	No
NotScheduled	Yes	Yes	Yes	No	No	Yes	No	No	No
Scheduled	No	No	Yes	No	Yes	Yes	No	No	No
WaitStarting	No	No	No	No	Yes	Yes	No	No	No
Running	No	No	No	No	Yes	No	No	No	Yes
Paused	No	No	No	No	Yes	No	No	Yes	No
Success	No	No	Yes	Yes	Yes	No	No	No	No
Failed	No	No	Yes	Yes	Yes	No	Yes	No	No
Committed	No	Yes	Yes	No	No	No	No	No	No
CommitFailed	No	No	Yes	Yes	No	No	No	No	No
Aborted	No	No	Yes	Yes	No	No	No	No	No
AbortFailed	No	No	Yes	Yes	Yes	No	No	No	No
PreloadPaused	No	No	No	No	Yes	No	No	Yes	No
Preloading	No	No	No	No	No	No	No	No	No
PreloadFailed	No	No	Yes	No	No	No	Yes	No	No
ResourceLocking	No	No	No	No	No	No	No	No	No
ResourceLockFailed	No	Yes	Yes	No	No	No	Yes	No	No

Device Group Task States and When to Perform Actions

The following matrix describes the different device task states and when you can perform actions on them.

States Below:	Action: Pause	Action: Resume	Action: Abort	Action: Submit	Action: Resubmit
Ready	No	No	No	Yes	No
ResetToReady	No	No	No	No	Yes
Running	Yes	No	Yes	No	No
Paused	No	Yes	Yes	No	No
Success	No	No	Yes	No	No
Failed	No	No	Yes	No	Yes
Rolledback	No	No	No	No	Yes
RollbackFailed	No	No	Yes	No	Yes
PreloadPaused	No	Yes	Yes	No	No
Preloading	No	No	No	No	No
PreloadFailed	No	No	No	No	Yes

7

Use an Offline Configuration for a Device Cluster

A common, top-level offline configuration template can be used to provision network function (NF) device cluster containing one or more groups that contain a device or a device high availability (HA) pair. An offline configuration can be created by making a copy of an existing configuration, packaged configuration, managed device configuration, or by selecting a schema from a supported software model.

> **Note:**
>
> For Oracle Enterprise products, offline configuration supports only the Enterprise Session Border Controller (ESBC).

Pre-packaged Offline Configuration Templates

The Oracle Communications Session Element Manager includes several pre-packaged offline configuration templates. Each template contains a base configuration for specific types of network environments.

> **Note:**
>
> For Oracle Enterprise products, pre-packaged offline configuration templates supports only the Enterprise Session Border Controller (ESBC).

Consider the following before you create an offline configuration:

- Create a detailed network topology map, including network domain information, such as slots, ports and networks, realms, and their relationships to each other.
- Identify device-specific parameters based on the topology map that later become offline configuration data variables.

Oracle Communications recommends that you make a copy of any packaged offline configuration template, so that you can continue to reuse the template for other domains that you may want to create. After you associate an offline configuration with a cluster of devices, the template is no longer available for other devices or clusters. The following table describes the packaged offline configuration templates.

Pre-packaged Offline Configuration	Network Application
SLRM_Standalone	• Access-hybrid IMS Oracle Communications Session Routers with subscriber-aware load balancing and route management (SLRM) systems, and Oracle Communications Session Border Controllers, and physical session routers (IMS Access Hybrid). • SLRMs only. • Core IP multi-media Subsystem (IMS), Oracle Communications Session Routers, and SLRMs (IMS Core).
CSM_HA	• High Availability (HA) IMS Core. • HA IMS Access Hybrid.
CSM_Standalone_SlrmLink	Standalone Oracle Communications Core Session Manager (CSM) configured to work with an SLRM.
CSM_HA_SlrmLink	An HA CSM that is configured to work with an SLRM.
ASBC_Standalone_SlbSlrmLinks	• Access standalone Oracle Communications Session Border Controllers (SBCs) • Subscriber-Aware Load Balancers (SLBs). • SLRMs. • IMS Access Hybrid.
ASBC_HA	Access SBCs for HA 3G to 4G mobile phone network.
SR_Standalone	Standalone SBCs.
SR_HA	HA SRs.
ASBC_HA_SlbSlrmLinks	Access SBCs for high-availability 3G to 4G mobile phone network with SLBs and SLRMs.
SLB_Standalone	• Standalone SLBs. • IMS-Access-Hybrid.

Add an Offline Configuration

You can either add an offline configuration by copying a managed device configuration or from an existing supported software schema in OCSEM.

Add an Offline Configuration from a Managed Device

You can seed a configuration from a from an existing managed device configuration.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. On the **Configuration Manager** slider, select **Configuration tools**, **Offline configurations**.

2. In the **Offline Config** tab, click **Add**.
3. In the **Add offline configuration** pane, complete the following fields:

Configuration name field	The unique configuration name that is an alphanumeric value from 1 to 24 characters with no spaces and no special characters with the exception of the hyphen (-) and underscore (_). **Note:** When you choose a name for a new global parameter configuration, this name must not start with the prefix "ID". A validation error (invalid oc name) occurs if the above rules are not followed.
Description field	The description for the configuration.
Offline configuration seeded from drop-down list	Select **Managed Device** to create an offline configuration by copying an existing managed device configuration.
Selected managed device field	Click the ellipsis (**...**) button to launch the **Select managed device** dialog to navigate to a device associated with OCSEM, and click **OK**. This field populates with the IP address of the device.

4. Click **Apply**.
5. In the **Success** dialog, click **OK**.

Load the new offline configuration and modify any of the pre-populated base parameters, as needed for your domain.

Add an Offline Configuration from a Software Version

You can seed a configuration from a supported software version schema.

Note:

For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. On the **Configuration Manager** slider, select **Configuration tools**, **Offline configurations**.
2. In the **Offline Config** tab, click **Add**.
3. In the **Add offline configuration** pane, complete the following fields:

Configuration name field	The unique configuration name that is an alphanumeric value from 1 to 24 characters with no spaces and no special

	characters with the exception of the hyphen (-) and underscore (_). **Note:** When you choose a name for a new global parameter configuration, this name must not start with the prefix "ID". A validation error (invalid oc name) occurs if the above rules are not followed.
Description field	The description for the configuration.
Offline configuration seeded from drop-down list	Select **Software version** to create an offline configuration from a supported software version schema.
Category	Click the ellipsis (**...**) button to select the plug-in product vendor category. For example, **SP Edge & Core** (for Service Provider (SP) Edge and Core products).
Component	The default NF component delivered by the plug-in product vendor category.
Platform drop-down list	Select the device hardware version to seed the configuration from a device template.
Supported software version drop-down list	Select the device software version in order to seed the configuration from a device template.

4. Click **Apply**.
5. In the **Success** dialog, click **OK**.

Load the new offline configuration and modify any of the pre-populated base parameters, as needed for your domain.

Add an Offline Configuration by Copying a Template

Use this task to copy an existing offline configuration or a pre-packaged offline configuration template to make a new offline configuration for your domain.

Note:

For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Configuration tools**, **Offline configurations**.

2. In the **Offline Config** tab, select an offline configuration template from the table, and click **Copy**.
3. In the **Copy Offline Configuration** dialog, enter the name of the new offline configuration.
4. In the **Success** dialog, click **OK**.

   The new offline configuration appears in the table.

Load the new offline configuration and modify any of the pre-populated base parameters, as needed for your domain.

Load an Offline Configuration

Use this task to configure, modify, and edit parameters for your offline configuration for your system domain.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. On the **Configuration Manager** slider, select **Configuration tools**, **Offline configurations**.
2. In the **Offline Config** tab, select the offline configuration that you want to use from the table, and click **Load**.
3. In the **Success** dialog, click **OK**.

   The system expands the configuration navigation tree under the **Offline Configurations** folder in the navigation pane. You can use this navigation tree to get to the required configuration elements.
4. Navigate the offline configuration and configure, modify, and edit parameters in your offline configuration.

Create Data Variables to Support Device Specific Values

Data variables can be created in the offline configuration, which are used to set device-specific values within the device cluster. Later when the offline configuration is applied to devices in the device cluster, the user is prompted to enter specific values for each parameter that is identified with a data variable.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. On the **Configuration Manager** slider, select **Configuration tools**, **Offline configurations**.

2. Load the offline configuration. See the Load an Offline Configuration section for more information.
3. Navigate to a configuration element in the navigation tree that is unique to an individual device. For example, IP address, Hostname, and so on.
4. When element attributes are rendered, click the data variable (DV) tool icon  in the upper right of the configuration body panel, and select an attribute to apply a data variable. A dialog appears if the targeted attribute supports DVs. The following table describes the required entries:

Selecting existing DV drop-down list	This list is populated if previous data variables where created. This feature allows the use of DVs that share the same values across different elements such as an IP address. You can select an existing DV for re-use so that all fields are populated with the same input value. If you are creating a new DV, keep the blank selection and enter a new entry by filling out other fields in this table. Select an existing DV to pre-populate the following parameters.
Name field	The an unique ID for the data variable. For example: **WANCOM2_UTIL_ADDR**
Label field	The name for the DV that appears in the individual Device configuration wizard later.
Description field	The description for the DV that appears in the tool-tip during configuration.
Default value field	The default value for the DV. **Note:** This value can be overwritten when you apply a template to a device.
Derive value check box	This box is not selected by default. Select the box to make the **Formula** field appear, so that the value for this DV is derived from the source information in the formula. **Note:** Deselecting this box makes the **Formula** field disappear.
Formula field	The formula contains the name of the DV (in brackets) that is being referenced by this DV. For example: HS_ROUTE = 'sip:${SIP_INT_IP}:${SIP_PORT}' The user is prompted for SIP_INT_IP (For example: 192.168.1.40) and SIP_PORT (For example: 5060), and the

	value of HS_ROUTE is derived automatically (For example: "sip:192.168.1.40:5060").

5. Click **Add**.
6. Click **Apply** to submit configuration changes.
7. In the **Success** dialog, click **OK**.
8. Repeat the previous steps to add more data variables to configuration elements in the offline configuration that are unique for each devices.

Edit the Offline Configuration

1. Expand the **Configuration Manager** slider and click **Configuration tools**, **Offline Configurations**.
2. In the **Offline Config** tab, select the offline configuration you want to edit from the table and click **Edit**.
3. In the **Edit offline configuration** dialog box, enter the description that you want for this offline configuration. If you are logged into Oracle Communications Session Delivery Manager as the Lawful Intercept (LI) administrator user, you can enter the LI encryption password for the LI configuration. Note that the LI encryption password parameter is not available for the Enterprise Edge and Core plug-in at this time.

> **Note:**
>
> You cannot edit the global parameter configuration name.

4. Click **OK**.

> **Note:**
>
> Upon installation of Oracle Communications Session Delivery Manager, if R226 compliance is enabled, the Lawful Intercept and SIPREC features and their attributes are hidden from view and are not configurable.

Configure a Device Cluster with an Offline Configuration

You add a device cluster, which can contain a single device group or multiple device groups and associate it with a single offline configuration that you added. All targeted devices in the device cluster must share the same software version, and platform.

Add a Device Cluster Network Function

Pre-requisite: If you are not using the default **Home** group to add a device cluster NF, you must specify a device group. See the Configure Device Groups section in the *Device Manager* chapter for more information.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices - Group View** pane, click **Add**.

3. In the **Select Network Function Type** dialog box select the plug-in product vendor type from the **Categories** table.

> **Note:**
>
> Other EM plugin product vendor types may also display in this table if they are installed in Oracle Communications Session Delivery Manager.

4. In the **Network Function Type** drop-down list, select the **Device Cluster** NF type and click **Continue**.
5. In the **Add Network Function: Device Cluster** dialog box, complete the following fields:

Network Function Name field	The Network Function (NF) name that you want to use for the component device(s) that you are configuring. For example, **msgNF**.
Description	The description of the NF. For example, "There is only one scalability group, which might contain eight MSG devices."
Component Type drop-down list	Select one of the following NF component types that you want to configure. **Note:** Only devices that match the chosen component type can be added to the device cluster NF. For example, the SP Edge & Core product plug-in has the following component types: • **SBC**—Oracle Communications Session Border Controller. • **SR**—Oracle Communications Session Router. • **SLB**—Oracle Communications Session Load Balancer. • **CSM**—Oracle Communications Core Session Manager. • **SLRM**—Subscriber-aware load balancing and route management (SLRM) mechanisms. • **MSG**— Oracle Communications Mobile Security Gateway (MSG).
Device Cluster Name field	The name of the device cluster group in this NF. For example: **msgCluster**
Redundancy Type drop-down list	Select the device cluster redundancy type: • **HA**—The cluster has high-availability (HA) capability. • **STANDALONE**—The cluster is standalone and does not have HA capability.

6. Click **Apply**.

   The NF now appears in the **Managed Devices** pane.

Associate the device cluster with its offline configuration.

Associate a Device Cluster with an Offline Configuration

Once you have added a device cluster to an NF, the device cluster must be associated with an offline configuration.

Pre-requisites: You must add an offline configuration before you associate the device cluster with an offline configuration. See the Add an Offline Configuration section for more information.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the device cluster that you want to associate with an offline configuration and click **Edit**.
3. In the **Associate Offline Configuration to NF Device Cluster** dialog box, view and complete the following fields:

Network Function	The NF to which this device cluster belongs.
Device Cluster	The empty device cluster group that you selected. For example: **CSM-core**
Offline Configuration drop-down list	Select the name of the offline configuration from the list of available offline configurations that is available (that is not currently in use) that the device cluster uses. This offline configuration is used to initiate devices (that are added later) to this device cluster. **Note:** The offline configuration may not display in the selection box under the following circumstances: • It is in use by another device cluster. • Its redundancy type does not match the type that is selected when the device cluster was created. • The pre-existing offline configurations are also filtered.
Synchronized Mode check box	The synchronized mode determines if the devices in the device cluster have their individual configurations kept in synchronicity with the configuration defined in the offline configuration as it changes over time. Check the check box to use the offline configuration for activating devices when they are added to the device cluster, and for all future configuration management of those devices to go through the offline configuration. Individual configuration management for synchronized devices becomes "read only."

	If the check box is left unchecked (Default), the offline configuration is used to activate devices only when they are added to the device cluster, and all future configuration management of those devices is maintained separately from the offline configuration.

4. Click **Apply**.

Add a Device to a Device Cluster

Now that you have associated a device cluster to its offline configuration you can add devices to the device cluster.

Pre-requisites: A device is eligible to be added to a device cluster if it meets the following criteria:

- The device must contain a platform and software version that matches the Offline Configuration.
- The device must be accessible through SSH over the network.
- The device has all required entitlements enabled, and licenses installed, as needed, to provide any services enabled by the Offline Configuration.

> **Note:**
>
> Ensure that any device that is added to the cluster is not currently being managed by OCSEM. If a device is being managed by OCSEM, remove it from OCSEM so that you can add it to the device cluster.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices - Group View** pane, select to expand the device cluster to which you are adding a device.
3. Select the device cluster and click **Add**.
4. In the **Add Device to scalability group** dialog box, complete the following fields:

Name	The device name.
Primary IP address field	The primary IP address for this device.
Secondary IP address field	The secondary IP address of the device. This field appears if you have a high-availability (HA) device pair only. Both FQDNs for the HA pair devices must be mapped to the corresponding IP addresses in the /etc/hosts file where OCSDM is installed.
User Name field	The device user name.
User Password field	The device password.
SNMP agent mode drop-down list	Select the SNMP version number that the SNMP agent supports and click **Load**. Valid versions are **v1**, **v2** and **v3**. If you select **v3**, authentication fields for SNMP

	version 3 appear. See below for more information about these fields.
SNMP port field	The SNMP port number. The default SNMP port number is 161.
SNMP community name field	**Note:** This field applies only to SNMP version 1 and 2. Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. **Note:** For a device cluster, the SNMP community name must match an SNMP community that is defined in the offline configuration, which must also contain the IP addresses of each SDM server cluster node.
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **SHA**—Secure hash algorithm (SHA-1). • **MD5**—MD5 hash algorithm. • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **DES**—Data encryption standard algorithm (DES) for the encryption of electronic data. • **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**
SNMPv3 privacy password field	The SNMP version 3 privacy password.

5. Click **Check Device** to verify that the device has the same software version that the offline configuration uses.
6. Click **Next** to configure the necessary data variables offered by the offline configuration.
7. In the next dialog box, enter the device-specific parameters for each data variable that you are provided (through the offline configuration).

> **Note:**
>
> See the Create Data Variables to Support Device Specific Values section for more information about how data variables are created in an offline configuration.

8. The device must already be active and on the network for the activation process to start (it has already booted). Click **Finish** to start the activation process.

   In the **Managed Devices** table, enable the hidden **Activation Status** column to see the device status. If the device activates successfully, the **Activated** status displays. If the device failed to activate, the **Activation Failed** status displays. For example, one scenario for a device that fails to activate could be if it was re-booted and failed to re-boot during the activation process.

Configure a Device Cluster Using a Bulk Spreadsheet

The OCSDM can provision a bulk device deployment using existing offline configurations and spreadsheets that contain required device details for the cluster.

Offline Configuration Spreadsheet Template

The first step in deploying a bulk device cluster is generating an offline configuration spreadsheet template.

To generate a spreadsheet template, you select an existing offline config from the **Offline Config** page and the OCSDM takes all of the headers and bind variables from this offline configuration and puts them into the generated template.

> **Note:**
>
> If the offline configuration from which you generated your template is changed after you have created your spreadsheet, you must regenerate the template. Anytime a change is made to an offline configuration, the OCSDM performs validation checks on all associated spreadsheets and marks any spreadsheets invalid that fail.

When you generate a template, the OCSDM automatically names the file using the following format:

```
OfflineConfigName_<SoftwareVersion>_<Platform>_<Timestamp>
```

You can change the template name when you save the file.

When you generate a template, the spreadsheet's top two rows are filled in automatically, with the first row containing the details of the Software, platform, and schema of the offline configuration in the following format:

```
Offline Config, <Offline Config Name>, Software version, <Software version
of the Offline Config>, Platform, <Platform of the Offline Config>, Schema
name <Schema name of the offline config>
```

The second row's header fields are generated depending on whether this is a SNMP v1v2 device or a SNMPv3 device. The following header rows appear in the second row, separated by commas, for an SNMPv1v2 device:

Header	Description	Required?
Device name	The name of the device to be added.	Yes
Primary IP address	The primary IP address of the device; this value must be a valid IP address.	Yes
Secondary IP address	The secondary IP address of the device; this value must be a valid IP address.	No
Username	The username for accessing the device.	Yes
Password	The password for accessing the device.	Yes
SNMP Port	The port for SNMP access; this must be a valid port and must be a numeric value.	Yes
SNMP Community	The SNMP community name present on the device; this must be a valid SNMP community and must contain a valid SDM IP address.	Yes
Synchronized mode	Indicates if the device is powered by the original offline configuration; this may be `true` or `false`.	No; the OCSDM uses the value configured at the cluster level
Bind variable ..<n> Name	Corresponds to the bind variables for the selected offline configuration; this value must be of the same type.	No

The following header rows appear in the second row, separated by commas, for an SNMP v3 device:

Header	Description	Required?
Device name	The name of the device to be added.	Yes
Primary IP address	The primary IP address of the device; this value must be a valid IP address.	Yes

Header	Description	Required?
Secondary IP address	The secondary IP address of the device; this value must be a valid IP address.	No
Username	The username for accessing the device.	Yes
Password	The password for accessing the device.	Yes
SNMP Port	The port for SNMP access; this must be a valid port and must be a numeric value.	Yes
SNMPv3 username	The SNMPv3 username.	Yes
SNMPv3 Authentication protocol	SNMPv3 authentication protocol: • HMAC384SHA5126 • HMAC192SHA2256 • NONE	Yes
SNMPv3 Authentication password	The SNMPv3 authentication password.	No
SNMPv3 privacy protocol	The SNMPv3 privacy protocol: • NONE • AES128	Yes
SNMPv3 privacy password	The SNMPv3 privacy password	No
Synchronized mode	Indicates if the device is powered by the original offline configuration; this may be `true` or `false`.	No; the OCSDM uses the value configured at the cluster level
Bind variable ..<n> Name	Corresponds to the bind variable for the offline configuration; this value must be of the same type.	No

Generate a Template

1. Expand the **Configuration Manager** slider, expand **Configuration tools**, and click **Offline Configurations**.
2. In the **Offline Config** page, select the offline configuration row to use for this spreadsheet and click **Generate Template**.
3. In your browser, a dialog box appears to either open or download the template file. Open the file, edit your spreadsheet as necessary, and save.

Deploy a Device Cluster Using a Bulk Spreadsheet

Once you have generated a template and entered all of the required device information into the spreadsheet, you can deploy and manage the device cluster using the **Device Manager**, **Bulk device deployment** page.

The **Bulk device deployment** page contains two tabs:

- OC spreadsheet—Allows you to upload, add, modify, delete, and edit offline configuration template spreadsheets.

- Bulk Device Deployment—Allows you to create, schedule, edit, start, and delete bulk device deployment work orders. You can also view logs and work order statuses.

Upload a Bulk Spreadsheet

Once you have generated a template and entered the required device information, you must upload it to OCSDM.

1. Expand the **Device Manager** slider and select **Bulk device deployment**.
2. In the **OC Spreadsheet tab**, click **Upload**.

   The **Upload OC bind variable spreadsheet** dialog box appears.
3. In the dialog box enter a new name for the spreadsheet, browse to the location of the file, and click **Upload**.

   Upon clicking **Upload**, the OCSDM checks the following conditions to ensure the file is valid:

   - The file is in csv format with .csv as a file extension.
   - The first row of the file is formatted properly. See "Generate a Template" for more information.
   - The file is associated with and properly matches an existing OCSDM offline config.
   - The spreadsheet does not contain any blank rows.
   - The spreadsheet contains details for no more than 20 devices.
   - The values corresponding to each header comply with the expected format.

If any of the validations fail, the upload fails displaying an error and the details are added to the log file.

Once a spreadsheet is validated successfully, you are returned to the **OC Spreadsheet** page with the new spreadsheet appearing in the table.

Manage Bulk Device Deployment Spreadsheets

You can access any successfully uploaded spreadsheets to view, edit, delete, and download them.

To manage bulk device deployment spreadsheets, expand the **Device Manager** slider and select **Bulk device deployment**. The OC Spreadsheet tab appears, listing all OC bulk spreadsheets successfully uploaded on the OCSDM.

The following information is displayed for each file:

File name	The name of the spreadsheet.
Offline Config	The offline config associated with this spreadsheet.
Software Version	The software version associated with this spreadsheet.
Platform	The platform of the associated offline config.

When you select a spreadsheet from the table by highlighting the row, the following buttons are enabled:

View	Displays a read-only version of the spreadsheet.

Edit	Displays an editable version of the spreadsheet, allowing you to make and save changes. **Note:** The OCSDM validates any values added or updated before updating the spreadsheet. • Add: Adds a new row to the spreadsheet. If the spreadsheet already has details for 20 devices, the OCSDM displays an error when you click this button. • Edit: The values from the selected row of the spreadsheet are displayed in a dialog you can modify. **Note:** The SNMP agent mode is read-only and cannot be modified. • Delete: Deletes a row in the spreadsheet. The OCSDM prompts you to confirm before deleting.
Delete	Deletes a spreadsheet. The OCSDM prompts you to confirm before deleting.
Download	Downloads the selected spreadsheet.

Overcoming the Limitations of Bulk Device Deployment

Bulk device deployment enables you to configure target SBCs using a file template created from an existing SBC with a similar hardware and software platform.

Limitations of the Bulk Device Deployment Process

The bulk device deployment or provisioning process replaces the security certificates and private keys of the target SBCs with the security certificate and private key of the source SBC that was used to create the Offline Configuration associated to the device cluster. Due to the replacement of the security certificates and private key, functionalities that require TLS connection (For example, ACP over TLS) will not function after the bulk device deployment is completed. This is limitation in the bulk device deployment process.

Overcoming the Limitations

The limitations of the bulk device deployment process can be overcome by modifying the process that SDM uses to configure target SBCs. The following process generated the limitation:

- Erase the existing configuration in the target SBCs to be added and configured by ‘bulk configuration’ or manual addition to the device cluster.
- Send the configurations in the Offline Configuration to the target SBC(s) and save the configuration.

This limitation can be overcome by modifying the above steps as:

1. SDM checks if the security certificate, tls-profile and the acp-tls-profile attributes in the system-configuration exists either in:
   - The Offline Configuration created from the existing SBC and associated to the device cluster.
   - The target SBCs to be added and configured in the device cluster.
2. If the Offline Configuration and the target SBCs to be added and configured in the device cluster do not contain security certificate, tls-profile and the acp-tls-profile attribute in the system-configuration, there is no change in the workflow.
3. If the Offline Configuration or the target SBCs to be added and configured in the device cluster, contain security certificate, tls-profile and the acp-tls-profile attribute in system-configuration, SDM needs to pull and save a copy of the security certificate, tls-profile and the acp-tls-profile attribute in the system-configuration of the target SBCs.
4. Erase the existing configuration in the target SBCs.
5. Modify the security certificate, tls-profile and the acp-tls-profile attribute in the system-configuration of the configurations created from the Offline Confirguration with the saved copy of the security certificate, tls-profile and the acp-tls-profile attribute in system-configuration of the target SBCs.
6. Sends and saves the modified configurations in the target SBCs. The security certificate, tls-profile and the acp-tls-profile attribute in the system-configuration in the Offline Configuration are not affected and are not considered for the creation of modified configurations which are sent and saved in the target SBCs.
7. Verify that the target SBCs are reachable and accessible by SDM. Ensure that the target SBC has been added to the Device Cluster.

Appropriate logs are created to log the operations performed in each of the above mentioned steps.

Manage Bulk Device Deployment Work Orders

The **Bulk Device Deployment** page allows you to manage bulk device deployment work orders.

The **Bulk Device Deployment** page is comprised of 2 tables, **Work orders** and **Device Details**.

The following table describes the Work order table's fields:

Name	The name of the work order.
Platform	The platform associated with the offline config.
Offline Config	The offline config for which the work order is created.
File name	The name of the offline config bind variable spreadsheet.
Device Cluster	The name of the Device Cluster associated to the offline config.
Status	The status of the work order. The following are valid values:

	• PartialConfigured: The work order was partially successful. • Notscheduled: The work order is not scheduled and a user must manually start it. • Scheduled:The work order is scheduled but has not started yet. • WaitStarting: A work order has been put into a run-waiting queue by a scheduler and waits for the scheduled start time. • Running: The work order has started and is running. • Success: The work order has completed successfully. • Failed: The work order failed. • StartAborting: The work order was created but a user has pressed the **Abort** button. • Aborting: The work order is executing the abort process. • Aborted: The work order has been aborted. All changes on the targeted devices are rolled back exactly as before the push task was executed. • AbortFailed: The work order failed to be aborted. • LockingResource: The work order attempts to lock all necessary resources. • LockResourceFailed: A work order has failed to lock all necessary resources.
Start time	The time the work order started or is scheduled to start.
End time	The time at which the work order completed, including both successful and unsuccessful completions.

The following table describes the Device Details table's fields:

Device Name	The name of the device as specified in the spreadsheet.
IP Address	The IP address of the device as specified in the spreadsheet.
Status	The status of the device after a work order has been executed. This value is either Success or Failure.

The following buttons are available to manage bulk device deployment work orders on the **Bulk Device Deployment** page:

Refresh	Refreshes the work order table.
Search	Search through work orders using pre-defined criteria.
Show All	Show all existing work orders associated with this bulk device deployment.
Logs	Opens a new window displaying the logs for the selected work order (if it has been executed).
Add	Creates a work order.
Start	Starts an already created work order; this button is only enabled when you have selected a row.

Edit	Allows you to edit certain details of a selected, existing work order.
View	Allows you to view the details of a work order.
Abort	Allows you to abort a work order that has started or is scheduled to start; this button is only enabled when you have selected a row.
Delete	Deletes a work order; you cannot delete a work order currently in progress.

Add a Work Order In a Bulk Device Deployment

You can add a new work order to an existing bulk device deployment.

1. Expand the **Device Manager** slider, select **Bulk device deployment**, and click the **Bulk Device Deployment** tab.
2. Click **Add**.
3. In the **Settings** pane, complete the following fields:

Name	The name of the work order; this must be an alphanumeric value and cannot contain spaces.
Scheduled	Indicate whether the work order is scheduled or not.
Start date and time	Select the date and time when the work order is to be executed; This field is enabled only when the **Scheduled** checkbox is checked.

4. In the **Offline Config Spreadsheet** pane, complete the following fields:

Device Cluster	The name of the device cluster for this work order.
Offline Configuration	The name of the associated offline configuration for this work order.
Offline Config Spreadsheet	The name of the offline config spreadsheet for this work order.

5. Click **Apply**.

Search For Work Orders

You can search for work orders using pre-defined criteria.

From the **Bulk Device Deployment** pane, click the **Search** button.
You can search for recordings based on the following criteria:

- Name
- Platform
- Device Cluster
- Offline Config
- Start time
- End time
- Status

8

Configure and Apply a Reusable Configuration Module

A Reusable Configuration Module (RCM) is a work flow template that describes a sequence of configuration changes that are used to deploy a feature on a device. An RCM can be applied without having to modify the top-level configuration elements because it targets specific parameters, and does not require a clustered device environment or a specific software version.

An RCM can use an existing device schema model and be associated with device configurations by inputting values for the specified variables. This abstracts the end user from the model schema, allowing for the configuration of specific functionality without knowledge of the element topology.

Oracle Communications Session Element Manager modifies the specified attributes in the target configuration to the values contained within the RCM.

> **Note:**
>
> An RCM can be applied to any supported Oracle Communications Session Delivery product device software model.

> **Note:**
>
> For Oracle Enterprise products, RCM supports only the Enterprise Session Border Controller (ESBC).

The following preexisting RCMs are included with Oracle Communications Session Element Manager:

Name	Description
rcmAddSLRMtoASBC	Adds an Oracle Communications SLRM to an Oracle Communications ASBC configuration.
rcmRemoveSLRMfromCSM	Removes an Oracle Communications SLRM from an Oracle Communications Core Session Manager configuration.
rcmRemoveSLBfromSBC	Removes an Oracle Communications Subscriber-Aware Load Balancer from an Oracle Communications Session Border Controller configuration.
rcmAddSLBtoSBC	Adds an Oracle Communications Subscriber-Aware Load Balancer to an Oracle Communications Session Border Controller configuration.

Name	Description
rcmAddSBCtoSR	Adds an Oracle Communications Session Border Controller to an Oracle Communication Session Router configuration.
rcmRemoveSLRMfromASBC	Removes an Oracle Communications SLRM from an Oracle Communications ASBC configuration.
rcmRemoveSBCfromSR	Removes an Oracle Communications Session Border Controller from an Oracle Communications Session Router configuration.
rcmAddSLRMtoCSM	Registers an Oracle Communications SLRM with an Oracle Communications Core Session Manager configuration.

Add a New Reusable Configuration Module from an Existing Software Model Schema

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider and select **Configuration Tools**, **Reusable Modules**.
2. In the **Reusable Configuration module** pane, click **Add**.

Name field	The unique name of the RCM.
Description field	The RCM description.
Modifiable drop-down list	Select from the following user permissions: • Select **public** to allow any user to modify this RCM. • Select **private** to allow only the creator of the RCM to modify this RCM.
Category field	Click the ellipsis (**...**) button to select the product plug-in vendor category: a. In the **Select network function type** dialog box, select the NF type. b. Click **Select**.
Component field	This field populates with **Default** (NF component) when the product plug-in vendor category is selected.
Platform drop-down list	Select the platform of the device software on which the RCM is based.

Supported software version drop-down list	Select the device software version on which the RCM is based.

3. Click **Apply**.

Add an Element to an Existing Reusable Configuration Module

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider and select **Configuration Tools**, **Reusable Modules**.
2. Select the RCM you want to modify, and click **Load**.
3. Select the element type row from the **Elements defined** table and click **Add**.
4. In the **Add Element** dialog box, complete the following fields:

Type drop-down list	(Required) Select the type of element to be defined.
Name field	(Required) Enter a unique name for the element action.
Description field	Enter a description for the element action.
Element action drop-down list	Select the configuration action for the targeted element. You can add an element to a configuration, modify an existing configuration element, or remove a configuration element. • An **ADD** element may not contain any sub-element with a **MODIFY** or **DELETE** action. • A **MODIFY** action cannot be performed on the parent of any configuration element that is part of an Order Group. • Required sub-elements cannot be removed from RCM elements with a top level **ADD** action. • A **MODIFY** or **DELETE** top-level element can only change into an **ADD** action if all its required sub-elements exist. • Select **ADD** to add an element if it is not found in the target work flow. • Select **MODIFY** to modify the element if it is found in the target work flow. • Select **DELETE** to delete the selected element if it is found in the target work flow.

> **Note:**
>
> The provisioning policy rules apply to each RCM action for each element instance level.

5. Click **Add Variable**.
6. In the the **Add element** dialog box, complete any element-specific parameters. See your product device documentation for more information about these parameters.
7. Click **Apply**.
8. Click **OK** to dismiss the confirmation dialog.

Modify Element Properties in an Existing Reusable Configuration Module

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. In the **Reusable Configuration module** table, select the RCM you want to modify, and click **Load**.
3. Select the element you want to edit in the **Elements defined** table, and click **Edit**.
4. Select the element you want to edit in the **Elements defined** table, and click **Modify definition**.

Description field	Enter a description for the element.
RCM action drop-down list	Select the configuration action for the targeted element. You can add an element to a configuration, modify an existing configuration element, or remove a configuration element. • An **ADD** element may not contain any sub-element with a **MODIFY** or **DELETE** action. • A **MODIFY** action cannot be performed on the parent of any configuration element that is part of an Order Group. • Required sub-elements cannot be removed from RCM elements with a top level **ADD** action.

- A **MODIFY** or **DELETE** top-level element can only change into an **ADD** action if all its required sub-elements exist.
- Select **ADD** to add an element if it is not found in the target work flow.
- Select **MODIFY** to modify the element if it is found in the target work flow.
- Select **DELETE** to delete the selected element if it is found in the target work flow.

> **Note:**
>
> The provisioning policy rules apply to each RCM action for each element instance level.

5. Click **Apply**.
6. Click **OK** to dismiss the confirmation dialog.

Predefine Variable Values for an Element in a Reusable Configuration Module

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. Select the RCM that you want to modify, and click **Load**.
3. Select the element you want to edit from the **Elements defined** table, and click **Edit**.
4. Enter a pre-defined input value for each attribute name.
5. Repeat until all required variables are defined.
6. Click **Apply**.
7. Click **OK**.

Apply a Reusable Configuration Module to a Device

1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. Select the RCM that you want to apply to a device, and click **Apply**.
3. In the **Apply RCM to configuration** pane that appears, select the ellipse icon (**...**) next to the **Select managed device** field.

4. In the **Select managed device** dialog box, navigate the desired folder structure to your device.
5. Select the device, and click **OK**.
6. In the **Apply RCM to configuration** pane, click **Next**.
7. In the Configure **RCM input variables** pane, configure the input parameters for your device and click **Finish** when you are done.

Manage Reusable Configuration Modules

View Reusable Configuration Modules

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. View the following **Reusable Configuration module** table columns for the listed RCM entries:

Name	The RCM name.
Description	The RCM description.
Last modified date	The date and time when the RCM was last changed.
DNM	Dependancy notification message (DNM). Note that this column is not used.
Created data	(Hidden) The date at which data was created for this RCM.
Created by	(Hidden) Indicates user who created the RCM. A preexisting RCM indicates **EM_SYSTEM**.
Category	(Hidden) The product plugin vendor category.
Component	(Hidden) The element manager (EM) plugin product NF component.
Schema version	(Hidden) The software model schema for devices.
Modifiable	(Hidden) Indicates the following permisions: • **public**— Any user can modify this RCM. • **private**—Only the creator of the RCM can modify this RCM.

Update a Network Function Device Configuration

Pre-requisites: You must apply the RCM to a device before you can save and activate changes. See the Apply an RCM to a Device section for more information.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Devices**.
2. In the **Managed Devices** table, navigate the folder hierarchy to the network function (NF) device, and click **Update**.
3. In the update dialog, choose from the following options:
   - (Default) Select **Save & activate configuration** to save the configuration and make the current working configuration on the device the running configuration.
   - Select **Save configuration** to save the current working configuration changes to the device.
   - Select **Activate configuration** to make the current working configuration the running configuration.

Delete an Element from an Existing Reusable Configuration Module

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

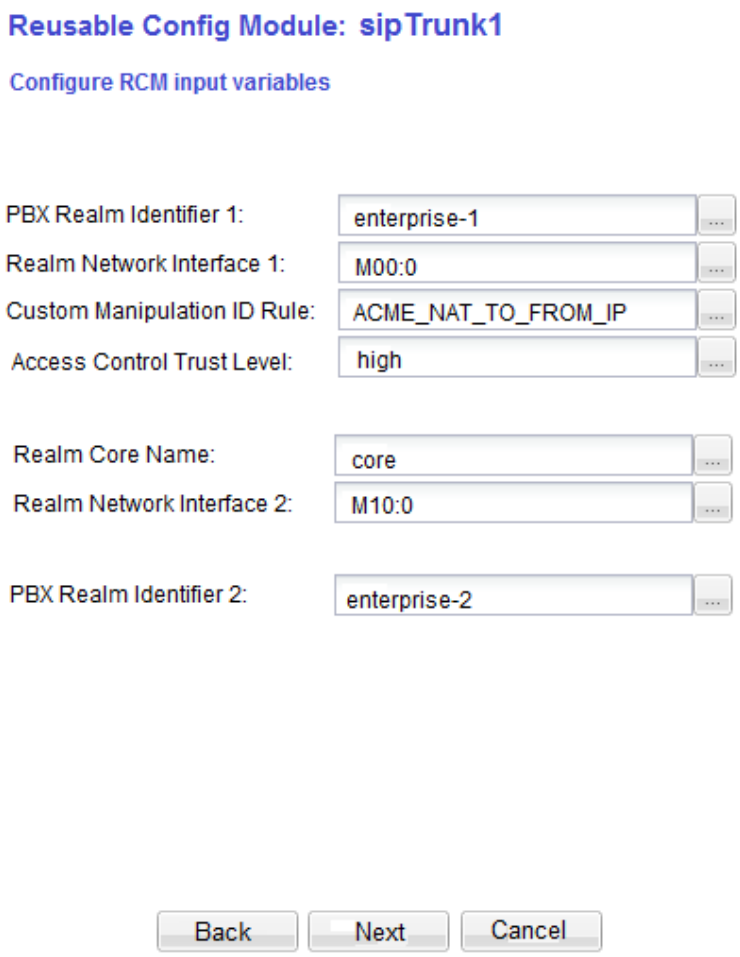
1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. Select the RCM, and click **Load**.
3. Select the element you want to delete from the **Elements defined** table, and click **Delete**.
4. In the confirmation dialog, click **OK**.

Reusable Configuration Module Input Wizard Configuration: Example

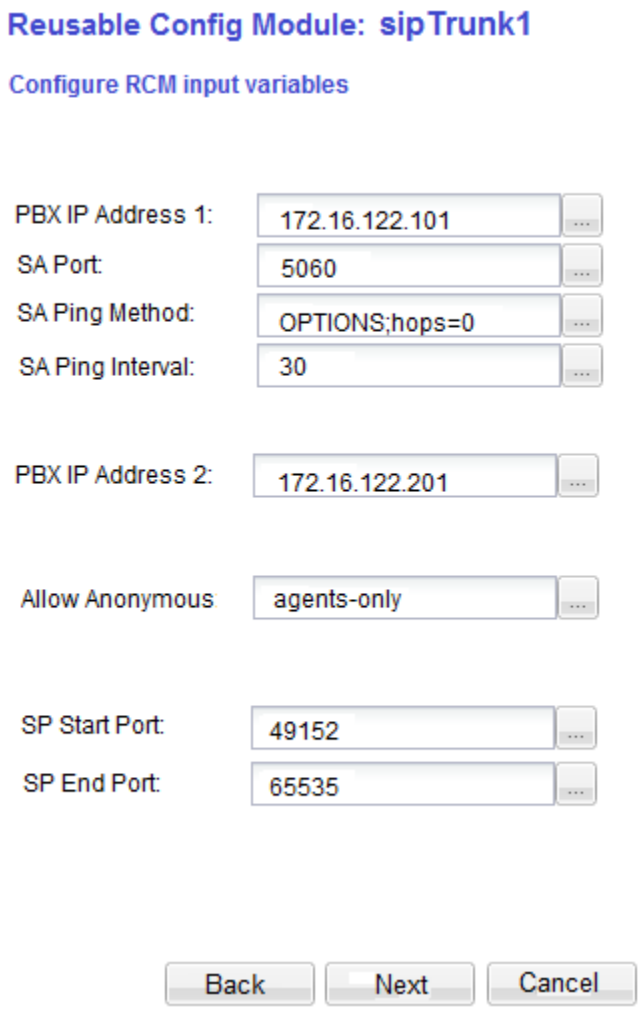
The following example shows how input values are entered in the **RCM Input wizard** screen for an SIP Trunk service RCM.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

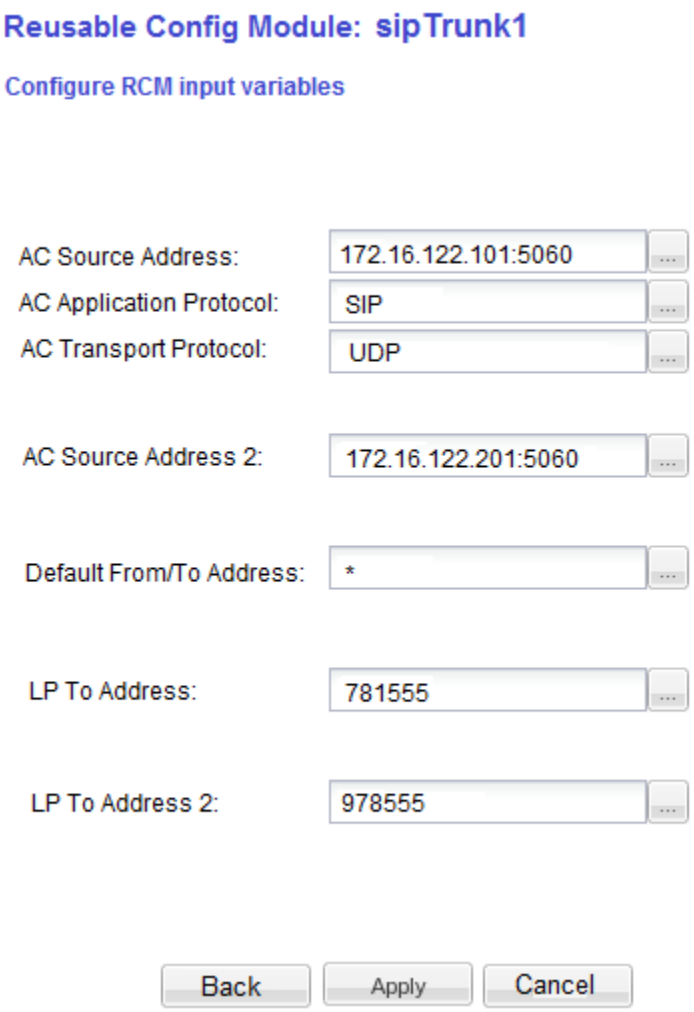
1. Enter values for all specified attributes and click **Next**.



2. Enter values for all specified attributes and click **Next**.



3. Enter values for all specified attributes and click **Apply**.



The configuration modifications are validated against the target device's data model schema.

Delete a Reusable Configuration Module

An RCM is deleted only if it is not assigned to any device or configuration with a dependency. When the RCM is deleted, it is permanently removed from the database and cannot be retrieved.

> **Note:**
>
> For Oracle Enterprise products, the following procedure supports only the Enterprise Session Border Controller (ESBC).

1. Expand the **Configuration Manager** slider, and select **Configuration Tools**, **Reusable Modules**.
2. In the **Reusable Configuration module** table, select the RCM you want to delete, and click **Delete**.
3. In the **Delete** confirmation dialog, click **Yes**.

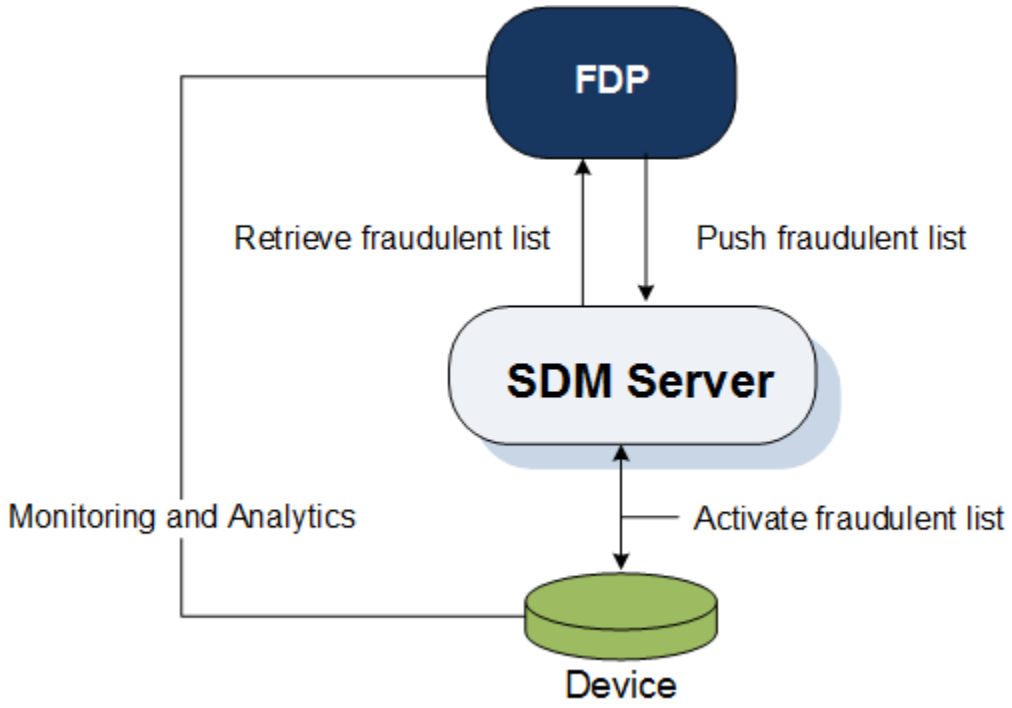
9
Fraud Protection Manager

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 9-1 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

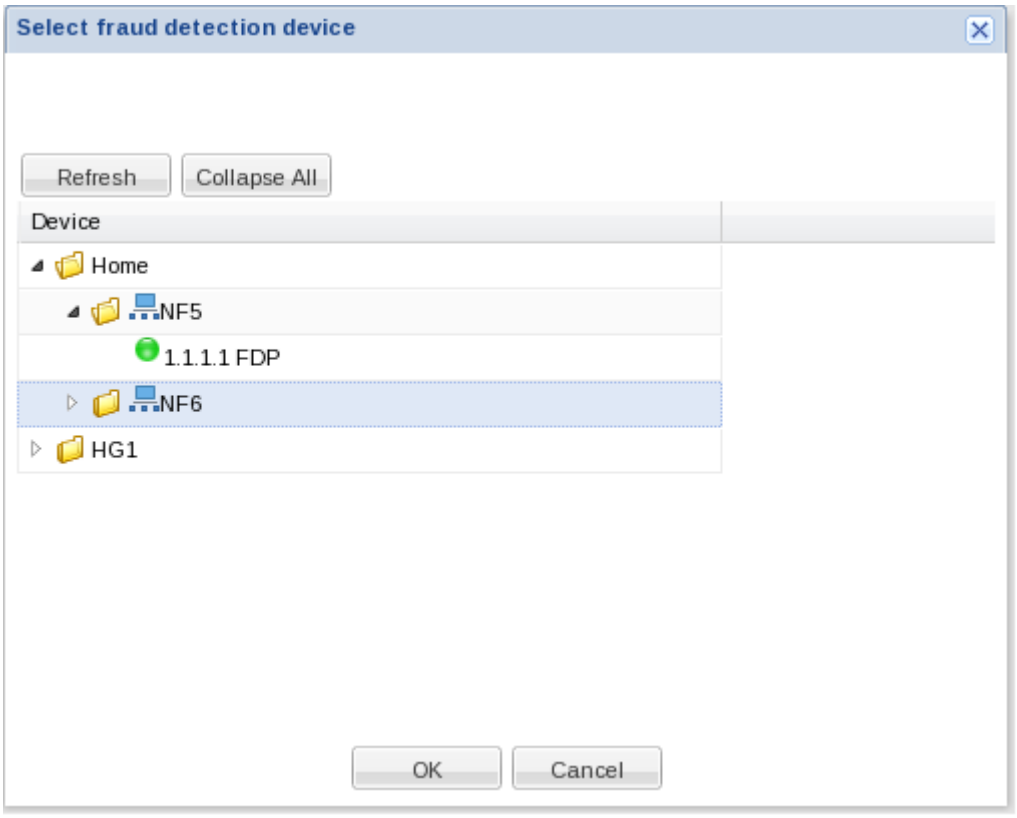
1. Expand the **Fraud Protection Manager** slider, and click **Administration**.
2. In the **Fraud Detection devices** pane, click **Add**.
3. In the **Add registration** dialog box, complete the following fields:

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	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**. You must add the folder structure, install the Enterprise Utilities plug-in, and specify the FDP network function (NF) type in Device Manager before you can select a FDP device.
Description field	The description of the FPD 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. Note that the user must have full Fraud protection list privileges. Use the following steps to set these privileges: 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	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: • **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: • **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	The following characters are allowed for a phone number: • 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. • Entries with + symbol are supported. No leading zero characters are allowed.

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. **Note:** The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.
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.

	Note: The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.
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. **Note:** The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.

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. **Note:** The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.

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. **Note:** The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.
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. **Note:** The name of the FPL file present on the southbound device must not contain any underscore (_) as it affects the Restoring Archived FPL functionality.
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.

5. Click **OK**.

Copy a Fraud Protection List Entry

You can copy values from one Fraud Protection List (FPL) entry to build a new 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 **Copy**:
   - **Black list**
   - **White list**
   - **Rate limit**
   - **Call redirect**
4. 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.

5. 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 *Updated successfully* or *Failed reconciliation* 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: • **Success** • **Updated successfully** • **Failed reconciliation** • **In Progress** • **Copy in Progress** • **FDP Update in Progress** • **FDP Update Failed** • **Export in Progess** • **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	Select from the following push task types: • **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	Select from the following push task types: • **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.

4. In the **Device group tasks** table and select the Network Function (NF) and click **Manage** to edit device in the push task.

5. 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.

6. 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	A push task can have the following status: • **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	The end time is the server local time when the following conditions occur for this push task: • 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.
Status	A device task can have the following status: • **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.

Name	Description
Start time	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: • 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	The end time is the server local time when the following conditions occur for this device task: • 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 alpha-numeric 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	You can filter on any of the following push task status entries: • **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	The end time is the server local time when the following conditions occur for this push task: • 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 **Committted** 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	Select from the following options to set the type configuration backups for devices: • **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. **Note:** The parameters described below are unavailable if you choose this option.
Frequency drop-down list	Select from the following options to set the frequency of configuration backups for devices: • **None**—Select to not repeat a scheduled backup. • **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: • **None**—Select to not repeat a scheduled backup. • **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 **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	**Please choose purge policy** radio-button options—Select one of the following purge policy options: • **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	Enter values for the following fields: • **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: • 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**.

10

Dashboard Manager

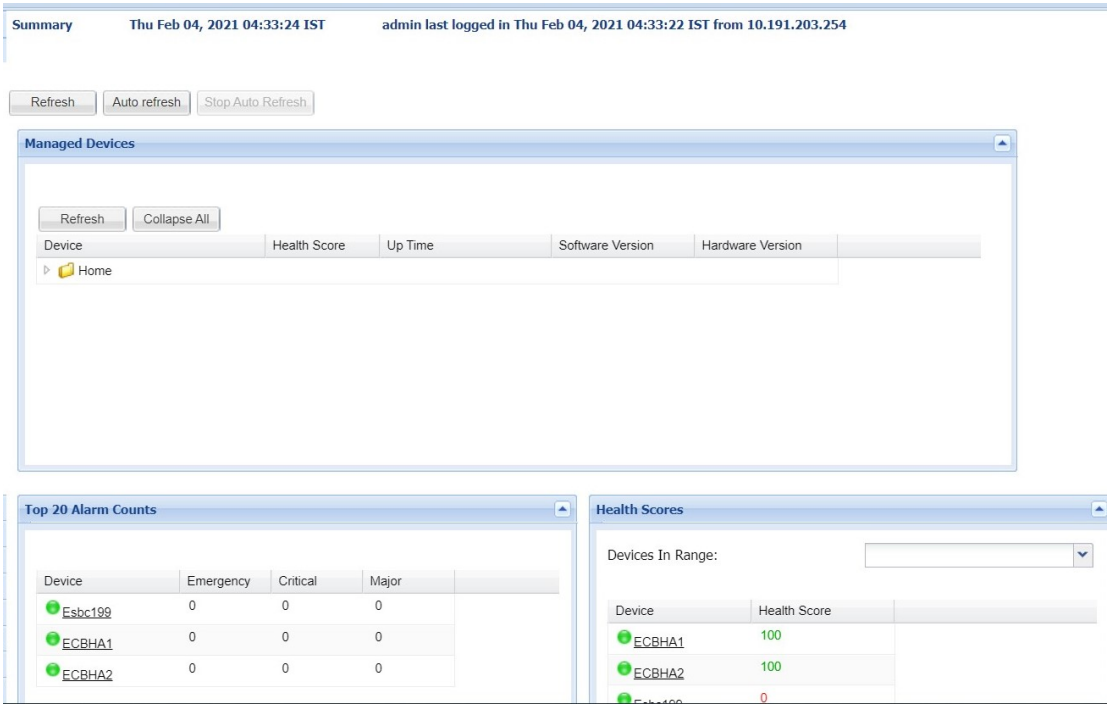
Dashboard Manager is used to view summary data, work orders, and sample health status information for devices.

> **Note:**
>
> You can also view (read-only) both work order types by selecting **Work Order View** from the **Dashboard Manager** slider. See the View Work Order Information chapter to view information for the work orders you configured for applying global parameters and software upgrades to targeted devices.

View Summary Data

The following summary data can include general SDM system-level information (for example,c the local date and time (with time zone adjustment) of the SDM server), key performance indicator (KPI) data, or data retrieved for NF devices managed by Oracle Communications Session Element Manager. When you expand the **Dashboard Manager** slider and select **Summary view**, the **Summary** pane displays summary information for all active and standby devices similar to what is shown in the following figure:

Figure 10-1 Dashboard Manager Summary View



The following portals are displayed:

- **Managed Devices**—A list of all managed devices by either IP address or host name.
- **Top 20 Alarm Counts**—Key performance indicators (KPI) for the alarm (fault) status summary for each device.
- **Health Scores**— Tabular data that represents the health score of devices. The health scores can be interpretted as:
  - 75-100 - Average to good health
  - 50 to 74 - Poor to average health
  - below 50 - Poor health.
- **Top 20 CPU Usage**—A list of the top 20 devices that display based on their CPU usage.
- **Top 20 Memory Usage**—A list of the top 20 devices that display based on their memory usage.
- **Top 20 Call Rate**—A list of the top 20 devices that display based on the number of calls and concurrent sessions on each device.
- **Logged In Users**—A list of users logged into SDM with session start times and locations (IP addresses).

Refresh Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. At the top of the **Summary** pane, click **Refresh** to update the whole dashboard summary view.

Configure Auto Refresh

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Click **Auto refresh**.
3. In the **Auto refresh** dialog box, enter the number of seconds for when the page contents update.
4. Click **OK**.

Stop Auto Refresh

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Click **Stop Auto Refresh** to cancel a configured auto refresh interval for when the page contents update.

> **Note:**
>
> This button appears when the auto refresh function is configured only.

View Managed Device Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Managed Devices** table, expand a device group folder(s) to navigate to the device you want to view.

Device	The managed device is underlined, which indicates you can select the device to view more summary data for this device. **Note:** You can hover your mouse and a pop-up displays with additional device data. A round colored icon next to each device displays whether the device can be reached: • **Green**—The device is reachable and information for this device can be retrieved through SNMP. • **Red**—The device cannot be contacted.
Health Score	The system health percentage, with a system health percentage value of 100 (100%) being the healthiest.
Up Time	The system up time in hours, minutes, and seconds.
Software Version	The full release version of the device, which includes its software revision.
Hardware Version	The full identification of the device hardware platform.

View Key Performance Indicator Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **Key Performance Indicators** table, the following information displays for your device:

Device	The device managed by Oracle Communications Session Element Manager and for which the data is retrieved through an SNMP query.
Location	The physical location for this managed device.
Up Time	The system up time for this device in days, hours, minutes, and seconds.
Health Score	The health score for this device. The health score range is 0 to 100. Health scores lower than 60 indicate the device is in poor health.
CPU	The percentage of CPU used in this device.

Memory	The percentage of memory used in this device.
Licensed Session Used	The number of concurrent calls from the system performance report and current signaling sessions.

3. Click **Refresh** to update KPI data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View Alarm Summary Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **Alarm Summary** area, you can see tabular data that displays the alarms summary data.
3. Click **Refresh** to update alarm summary data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View License Information

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **License Information** table, the following information displays for your device:

License Key	The license number for this device.
License Capacity	The maximum number of simultaneous sessions allowed by the device for all combined protocols.
Install Date	The device installation time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if license is not enabled.
Start Date	The start time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if the license is not enabled.
Expiration Date	The expiration time and date in the following format: hh:mm:ss, month, day, year and displays N/A if the license is not enabled.
Features	The features licensed for this device. For example, some licensed features may include: • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG)

	• ACC (Allows the device to create connections and send CDRs to one or more RADIUS servers.) • High Availability (HA)
Protocols	The protocols licensed for this device. For example, some licensed protocols may include: • SIP • MGCP • H.323

3. Click **Refresh** to update license data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View Health Score Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Health Scores** dialog box, you can view the health score percentage ranges for your devices or see individual devices in the **Device** list to display additional data for each device.
3. In the **Health Scores** dialog box, use the **Devices in Range** drop-down list to select the range of devices for which you want to view health scores:
   - **View All**
   - **75-100**—Average to good health.
   - **50-74**—Poor to average health.
   - **0-49**—Poor health.

View Top 20 Memory Usage

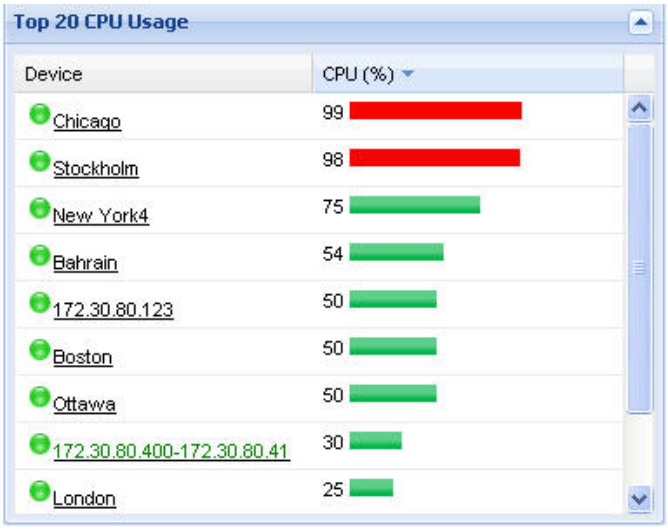
1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 Memory Usage** dialog box, a summary of the top 20 devices currently using the most memory the table is sorted by the descending percentage of memory. Mouse over each device to see additional information.

   The **Memory Usage** column displays the percentage of the memory utilization, followed by a colored bar, which corresponds with the memory usage percentage. The greater the percentage, the longer the bar. A red bar indicates a warning that memory usage is between 90% and 100% and a green bar indicates memory usage is below 90%.

View Top 20 CPU Usage

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 CPU Usage** dialog box, a summary of the top 20 devices with the most current percentage of CPU utilization is sorted by the descending percentage of CPU utilization. Mouse over each device to see additional information.

The **CPU (%)** column displays the percentage of the CPU utilization, followed by a colored bar, which corresponds with the CPU usage percentage. The greater the percentage, the longer the bar. A red bar indicates a warning that CPU usage is between 90% and 100% and a green bar indicates memory usage is below 90%.

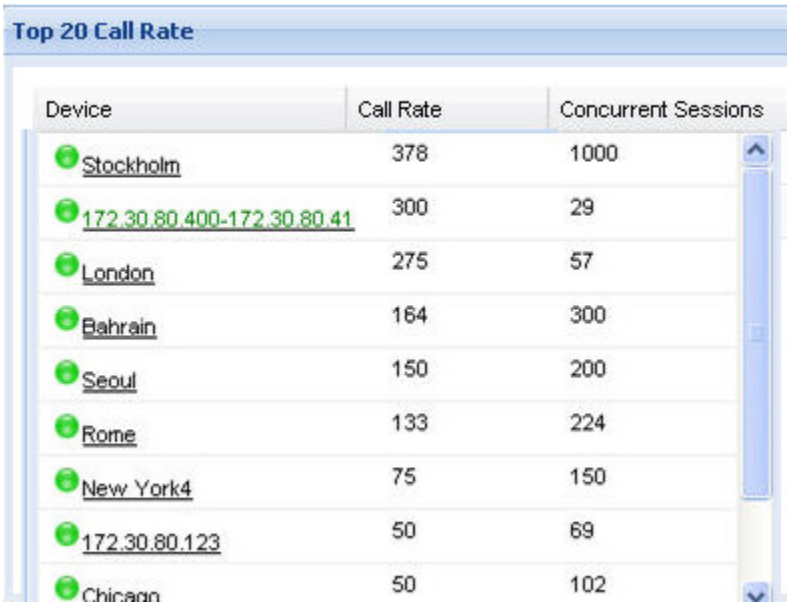


View Top 20 Alarm Counts

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 Alarm Counts** dialog box, a summary of the top 20 devices with generated alarms that include **EMERGENCY**, **CRITICAL** and **MAJOR** designations. You can position your mouse over each device to see additional information for the device.

View Top 20 Call Rate

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Expand the Dashboard Manager slider and click **Summary View**.
3. In the **Top 20 Call Rate** dialog box, a summary of the top 20 devices with highest number of active calls and concurrent sessions for each device. Mouse over each device to see additional information. For example:



View Logged In Users

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Logged In Users** dialog box, a summary of users logged into Oracle Communications Session Delivery Manager with the appropriate privileges is sorted in ascending alphanumeric order by default with the IP address of the user system.

> **Note:**
>
> The list does not display if you do not have administration-level privileges.

11 Performance Manager

The **Performance Manager** slider has a navigation pane that contains a set of performance groups (that appear when an device is selected) that can be accessed to get different kinds of statistical and state information for your managed Oracle Communications Session Element Manager network functions (NFs) and their associated device(s) or device clusters.

Performance Manager collects and analyses data received or sent over NF over time by its software (through SNMP MIBs). This statistical and state data is displayed on-demand when you access a performance group. Information for this performance group is displayed in the **Performance Manager** pane. Use this chapter to find information for each performance group.

> **Note:**
>
> The SNMP community parameter must be configured for product devices from which performance data is being viewed. See the *Configuration Manager* chapter for more information.

View Performance Groups for a Device

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, select and expand a device group folder. The **Managed Devices** pane displays the following columns for each device:

Name	The descriptive name of the device.
Version	The software version running on the device.
Platform	The hardware version of the device.
Object ID	(Hidden) The internal database object identifier.
IP Address/ FQDN	Details of the devices added using IP or FQDN.

> **Note:**
>
> The default device group folder is **Home**.

3. Select a device in the device group folder, and click **View**.

   The **Performance Groups** folder appears with its performance groups in the navigation pane below the expanded **Performance Manager** slider.

> **Note:**
>
> If you click a performance group and do not select a device, statistics for the last device are loaded when you click **View**.

4. Select the performance group you want.

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the individual performance groups described in this chapter. See your device product documentation for more information. When you access a performance group data for devices that belong to a cluster, data for these devices appears in the content area. The title of each panel is the device name (or IP address) of each device in the cluster.

Save Performance Group Data

You can save performance group data that belongs to a device to a text file in comma separated values (CSV) format.

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Save to file**.
6. In the browser dialog box used to save the file, select the save the file option (for example, in Firefox, select **Save File**).

> **Note:**
>
> The saved file is saved in the following format:

```
<stats screen name>-<tab name>-<date> <hh-mm-ss>.csv
```

For example:

```
System-General-2011-06-10 13-53-21.csv
```

7. Click **OK** to save the file to your local directory and close the window.

Refresh Performance Group Data

Use the following sections to refresh the statistics displayed for a performance group that belongs to a device.

Refresh a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Refresh**.

Configure the Automatic Refresh Interval for a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Auto refresh**.
6. In the **Auto Refresh** dialog box, enter the number of seconds you want to configure for the auto refresh of performance data from this device performance group.
7. Click **OK**.

Stop the Automatic Refresh of a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Stop auto refresh**.

   The automatic refresh function of performance data stops.

A

Performance Group Reference

The following sections describe the types performance group data that can be viewed for a device in Performance Manager.

To navigate to a device performance group, see the *View Performance Groups for a Device* section in the *Performance Manager* chapter.

> **Note:**
>
> The information displayed for each performance group in this reference appendix serves as an example for any given session delivery product device. The information for each performance group depends on your session delivery product device and its version, which may be different or more current than the information found in the examples in this appendix. See your session delivery device product documentation for more information.

System

System: General Tab

CPU utilization (%)	The total percentage of CPU utilization measured in one second.
CPU Application load rate	The average load rate of the service applications taken over a period of up to 10 seconds.
Memory utilization (%)	The percentage of memory utilization.
CAM utilization (%) - media	The percentage of network address translation (NAT) table (in content addressable memory (CAM)) utilization.
CAM utilization (%) - ARP	The percentage of address resolution protocol (ARP) table (in CAM) utilization.
License capacity	The percentage of licensed sessions currently in progress.
Health score (%)	The system health percentage (a value of 100 (percent) is the healthiest).
Redundancy state	The information about the state of each device in an HA pair. Values are: • **active** • **standby**

Current signaling sessions (SIP, H.323, and MGCP)	The total number of global concurrent sessions at the moment.
Current signaling rate (SIP, H.323, and MGCP) (CPS)	The number of global calls per second.
I2C bus state	State of the environmental monitor located in the chassis. The values are: • **online**—Denotes regular call processing. • **offline**—Denotes no call processing but other administrative functions are available.

Identification Tab

System name	The administratively-assigned name for this node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
System contact	The text identification of the contact person for this node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.
System location	The physical location of this node. If the location is unknown, the field is left blank.
System description	The text description of the entity. This value includes the full name and version identification of the system's hardware type, software operating-system, and networking software.
System objectID	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed.
System uptime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

SNMP

SNMP Pane

General SNMP Data

Authentication traps	The SNMP entity is permitted to generate authenticationFailure traps.
In packets	The total number of messages delivered to the SNMP entity from the transport service.
Out packets	The total number of SNMP messages passed from the SNMP protocol entity to the transport service.

SNMP Inbound Details

Bad versions	The total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
Bad community names	The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
Bad community uses	The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASN parse errors	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
Silent drops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity that were silently dropped. They were dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
Too bigs	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.
No such names	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
Bad values	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
Read only	The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. **Note:** Generating an SNMP PDU that contains the value readOnly in the error-status field is a protocol error. This value is provided to detect incorrect implementations of SNMP.
General errors	The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Total requested variables	The total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
Total set variables	The total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP set-Request PDUs.
Get requests	The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity.

Get next requests	The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity.
Set requests	The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.
Get responses	The total number of SNMP Get-Responses that have been accepted and processed by the SNMP protocol entity.
Traps	The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity.

SNMP Outbound Details

Too bigs	The total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is tooBig.
No such names	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is noSuchName.
Bad values	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is badValue.
General errors	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is genErr.
Get responses	The total number of SNMP Get-Responses generated by the SNMP protocol entity.
Traps	The total number of SNMP Trap PDUs generated by the SNMP protocol entity.

IP

IP: General Tab

Total datagrams received	The total number of input datagrams received from interfaces, including those received in error.
Forwarding capability	This indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a badValue response if a management station attempts to change this object to an inappropriate value.
Default time-to-live	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
Reassembly timeout(s)	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.

Reassemblies required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembled datagrams	The number of IP datagrams successfully re-assembled.
Fragmented datagrams	The number of IP datagrams that have been successfully fragmented at this entity.
Fragmentation failures	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set).
Created due to fragmentation	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
Routing discards	The number of routing entries that were discarded although they were valid. A reason for discard could be to free up buffer space for other routing entries.

Inbound Details

Delivered	The total number of input datagrams successfully delivered to IP user-protocols including Internet Control Message Protocol (ICMP).
Header errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Address errors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example., 0.0.0.0) and addresses of unsupported Classes (for example., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). **Note:** This counter does not include any datagrams discarded while awaiting re-assembly.

Outbound Details

Requests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

	Note: This counter does not include any datagrams counted in ipForwDatagrams.
Discards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). **Note:** This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
No routes	Number of IP datagrams discarded because a route could not be found to transmit them to their destination. **Note:** This counter includes any packets counted in ipForwDatagrams which meet this no-route criterion. This includes any datagrams which a host cannot route because all of its default gateways are down.

Addresses Tab

IP Address	The IP address to which this entry's addressing information pertains.
Interface Index	The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
Network mask	Subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0.
Broadcast address	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value is 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.

Max reassembly size	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

Interface Stats Tab

Index	The unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization.
Name	The interface name.
Description	The text string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the hardware interface.
Type	The information about the type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.
MTU	The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface
Speed	The estimate of the current bandwidth of the interface in bits per second. For interfaces which do not vary in bandwidth or for those where an accurate estimation cannot be made, it contains the nominal bandwidth.
Physical address	The address of the interface at the protocol layer immediately below the network layer in the protocol stack. For interfaces which do not have such an address (for example, a serial line), it contains an octet string of zero length.
Admin status	Current administrative state of the interface. The values are: • **up** • **down** • **testing**
Operational status	Current operational state of the interface. The values are: • **up** • **down** • **testing**
Last change time	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value.
In octets	The total number of octets received on the interface, including framing characters.

Unicast packets in	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Non-unicast packets in	The number of non-unicast (for example, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
In discards	The number of inbound packets which were chosen to be discarded although no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
In unknown protocols	For packet-oriented interfaces, the number of packets received through the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.
Out octets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Unicast packets out	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Non-unicast packets out	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Out discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out errors	The number of outbound packets that could not be transmitted because of errors.

Interface Stats Utilization Tab

Name	The text string containing the name of the media interface. The name is the one assigned by the local device that can be a text name or a port number, depending on the interface naming syntax of the device.
Rx Utilization	The receive media ports that are used for media ports indexed by IF index.
Tx Utilization	The transmit media ports that are used for media ports indexed by IF index.

Extended Interface Stats Tab

Name	The text string containing the name of the interface. The name is the one assigned by the local device. It could be a text name or a port number, depending on the interface naming syntax of the device.

In

Multicast packets	The number of packets delivered from this layer to a higher layer that were addressed to a multicast address. For a MAC layer protocol, it includes both group and functional addresses.
Broadcast packets	The number of packets delivered by this layer to a higher level that were addressed to a broadcast address.

Out

Multicast packets	The number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent.
Broadcast packets	The number of packets higher-level protocols requested to be transmitted that were addressed to a broadcast address at this layer, including those discarded or not sent.

HC In

Octets	The total number of octets received on the interface, including framing characters.
Unicast packets	The number of packets delivered by this layer to a higher layer that were not addressed to a multicast or broadcast address at this layer.
Multicast packets	The number of packets delivered by this layer to a higher layer that were addressed to a multicast address at this layer. For a MAC layer protocol, this includes both group and functional addresses.
Broadcast packets	The number of packets delivered by this layer to a higher layer that were addressed to a broadcast address at this layer.

HC Out

Octets	Total number of octets transmitted out of the interface, including framing characters.
Unicast packets	Total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this layer; including those discarded or not sent.
Multicast packets	The total number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent. For a MAC layer protocol, this includes both the group and functional addresses.

Broadcast packets	The total number of packets that higher-level protocols requested be transmitted that were addressed to a broadcast address at this layer; including those discarded or not sent.
Link up/down trap enable	This field indicates whether linkUp/linkDown traps should be generated for this interface. The value should be enabled(1) for interfaces that do no operate on top of any other interface and disabled(2) otherwise.
High Speed	The estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If a value of n is reported, the speed of the interface is in the range of n-500,00 to n+499,999. For interfaces that do no vary in bandwidth or for those where no accurate estimation can be made, a nominal bandwidth is given.
Connector Present	If the interface layer has a physical connector, the value is true(1). Otherwise it is false(2).

ICMP Tab

Inbound Statistics

Messages	The total number of ICMP messages which the device received. **Note:** This counter includes all those counted by icmpInErrors.
Errors	The number of ICMP messages which the device received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
Destination unreachables	The number of ICMP Destination Unreachable messages received.
Time exceeded	The number of ICMP Time Exceeded messages received.
Parameter problems	The number of ICMP Parameter Problem messages received.
Source quenches	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.
Echoes	The number of ICMP Echo (request) messages received.
Echo replies	The number of ICMP Echo Reply messages received.
Timestamps	The number of ICMP Timestamp (request) messages received.
Timestamp replies	The number of ICMP Timestamp Reply messages received.

Address masks	The number of ICMP Address Mask Request messages received.
Address mask replies	The number of ICMP Address Mask Reply messages received.

Outbound Statistics

Messages	The total number of ICMP messages which the Oracle Communications Session Delivery product attempted to send. This counter includes all those counted by icmpOutErrors.
Errors	The number of ICMP messages which the Oracle Communications Session Delivery product did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
Destination unreachables	The number of ICMP Destination Unreachable messages sent.
Time exceeded	The number of ICMP Time Exceeded messages sent.
Parameter problems	The number of ICMP Parameter Problem messages sent.
Source quenches	The number of ICMP Source Quench messages sent.
Redirects	The number of ICMP Redirect messages sent.
Echoes	The number of ICMP Echo (request) messages sent.
Echo replies	The number of ICMP Echo Reply messages sent.
Timestamps	The number of ICMP Timestamp (request) messages sent.
Timestamp replies	The number of ICMP Timestamp Reply messages sent.
Address masks	The number of ICMP Address Mask Request messages sent.
Address mask replies	The number of ICMP Address Mask Reply messages sent.

Global TCP Tab

Retransmission algorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
Retransmission timeout min (ms)	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre, an object of this type has the semantics of the LBOUND quantity described in RFC 793.
Retransmission timeout max (ms)	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined

	semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre, an object of this type has the semantics of the UBOUND quantity described in RFC 793.
Max connections	The total number of TCP connections the Oracle Communications Session Delivery product supports. In entities where the maximum number of connections is dynamic, this object contains the value -1.
Active opens	The number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Passive opens	The number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
Attempt fails	The number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state.
Established resets	The number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Current established	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
In segments	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Out segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Retransmitted segments	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
In errors	The total number of segments received in error (for example, bad TCP checksums). Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.
Out resets	The number of TCP segments sent containing the RST flag. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.

TCP Tab

Local address	The local IP address for this TCP connection. In the case of a connection in the listen state, the value is 0.0.0.0
Local port	The local port number for this TCP connection.
Remote address	The remote IP address for this TCP connection.
Remote port	The remote port number for this TCP connection.
State	The state of this TCP connection. Valid values are:

	• **closed** • **listen** • **established**

Global UDP Tab

In datagrams	The total number of UDP datagrams delivered to UDP users.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.
In errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Out datagrams	The total number of UDP datagrams sent from this device.

UDP Tab

Local address	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.
Local port	The local port number for this UDP listener.

Environmental

Voltage Tab

Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Voltage type	Value which indicates the sensor monitoring voltage. Values are: • v2p5- 2.5v sensor. This monitors L3 cache core voltage, micro-processor and co-processor I/O voltage, and Field-Programmable Gate Array (FPGA) memories I/O voltage. • v3p3 - 3.3V sensor. This monitors general TTL supply rail, control logic, micro-processor; micro-processor and co-processor; and SDRAM voltage. • v5 - 5V sensor. This monitors fans and micro-processor core voltage regulator. • CPU sensor. This monitors CPU voltage and micro-processor core voltage.
Description	The description of the entity being monitored for voltage. Values are: • 2.5V voltage (millivolts)

	• 3.3V voltage (millivolts) • 5V voltage (millivolts) • CPU voltage (millivolts)
Current voltage (millivolts)	The current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value.
Sensor state	The current state of the voltage for the device being monitored. Values are: • Host Processor 7450 and 7455 • normal range: 1.55v to 1.65v • minor range: 1.4v to 1.55v or 1.65v to 1.8v • shutdown range: <1.4v or >1.8v • Host Processor 7457 • Version 1.0 • normal range: 1.35v to 1.45v • minor range: 1.00v to 1.35v or 1.45v to 1.6v • shutdown range: <1.0v or >1.6v • Version 1.1 and later • normal range: 1.25v to 1.35v • normal range: 1.25v to 1.35v • minor range: 1.00v to 1.25v or 1.35v to 1.6v • shutdown range: <1.0v or >1.6v
Slot ID	The slot on which this voltage is found.
Slot type	The type of module found in this slot.

Temperature Tab

Index	A monotonic, increasing number. When this number reaches the maximum value, the agent wraps the value back to 1.
Temperature source	The entity being monitored for temperature.
Description	A description of the temperature being monitored.
Current temperature (degrees Celsius)	The current temperature of the main board PROM in Celsius.
Sensor state	Current state of the temperature which can have one of the following values: • **initial**—The temperature is at its initial state.

	• **normal**—The temperature is normal. • **minor alarm**—The temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius. • **major alarm**—The temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius. • **critical alarm**—The temperature is greater than 73 degrees Celsius. • **shutdown**—The system should be shutdown immediately. • **not present**—The temperature sensor does not exist. • **not functioning**—The temperature sensor is not functioning properly. • **unknown**—Information cannot be obtained because of an internal error.
Slot ID	The slot on which this temperature is found.
Slot type	The type of module found in this slot.

Fans Tab

Index	A monotonic, increasing number. When this number reaches the maximum value, the agent wraps the value back to 1.
Location	Location of the fan. Values are: • **left fan** • **middle fan** • **right fan**
Description	The description of the fan. Values are: • **fan 1** • **fan 2** • **fan 3**
Current speed (% or range)	The current fan speed percentage.
Fan state	The current fan speed state. Values are: • **initial**: fan speed is at its initial state • **normal**: fan speed is normal • **minor**: fan speed is between 75% and 90% of the full fan speed • **major**: fan speed is between 50% and 75% of the full fan speed • **critical**: fan speed is less than 50% of the full fan speed • **shutdown**: system should be shutdown immediately

	• **not present**: fan sensor does not exist • **not functioning**—The fan sensor is not functioning properly. • **unknown**—Information cannot be obtained due to an internal error.
Slot ID	The slot in which this fan is found.

Power Supplies Tab

Index	A monotonic, increasing integer. When it reaches the maximum value, the agent wraps the value back to 1.
Location	The location of the power supply. Values are: • Left power supply (A) • Right power supply (B)
Description	The description of the power supply. Values are: • Power supply (A) • Power supply (B)
State	The current state of the power supply. Values are: • **normal**—The power supply is normal. • **unknown**—The power supply sensor does not exist.

Cards Tab

Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Type	The location of the phy card. Values are: • left phy card (Phy 0) • right phy card (Phy 1)
Description	Description of the phy card. Values are: • Phy 0 for the left phy card • Phy 1 for the right phy card
State	The current state of the phy card. Values are: • **normal**—The state of the phy card is normal. • **unknown**—The phy card is not present.

Realms

The following sections describe the realms performance group data that can be viewed for a Oracle Communications Session Element Manager device.

Current Details Tab

Index	A monotonic increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1
Name	The name of the realm for which the following statistics are being calculated.
Status	The current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.
Inbound active	The number of current active inbound sessions.
Inbound active session rate	The current inbound session rate in CPS.
Outbound active sessions	The number of current active outbound sessions.
Outbound current sessions rate	The current outbound session rate in CPS.
Inbound admitted	The total number of inbound sessions during the period.
Inbound not admitted	The total number of inbound sessions rejected due to insufficient bandwidth.
Outbound admitted	The total number of outbound sessions during the period.
Outbound not admitted	The total number of outbound sessions rejected because of insufficient bandwidth.
Short sessions	The lifetime number of sessions whose duration was less than the configured short session duration.

Average Period/State Tab

Index	A monotonic, increasing number. When this number reaches the maximum value, the agent wraps the value back to 1.
Name	The hostname of the realm for which the following statistics are being calculated
Status	The current status of the specified realm, which is expressed as INS, constraintsviolation, or callLoadReduction.
Inbound high current	The highest number of concurrent inbound sessions during the period.

Inbound average session rate	The average rate of inbound sessions during the period in CPS.
Outbound high current	Highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered sessions	The total number of answered sessions during the period.
Answer/Seizure ratio	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
Average latency	The average observed one-way signaling latency during the period in milliseconds.
Max latency	The maximum observed one-way signaling latency during the period in milliseconds.

Monthly Minutes Tab

Index	A monotonic, increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
Realm name	The name of the realm for which the following statistics are being calculated.
Realm status	Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.
Minutes left	The number of monthly-minutes left in the pool per calendar month for a given realm.
Minutes rejected	The number of rejected calls due to monthly-minutes constraints exceeded.

QoS Tab

Index	A monotonic increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
Realm name	The name of the realm for which the following statistics are being calculated.
Realm status	The current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.

Period average	The average QoS factor observed during the period.
Period maximum	The maximum QoS factor observed during the period.
Period exceeded major	The peg counts the number of times the major Rfactor threshold was exceeded during the period.
Total exceeded major	The peg counts the number of times the major Rfactor threshold was exceeded during the lifetime.
Period exceeded critical	The peg counts the number of times the critical Rfactor threshold was exceeded during the period.
Total exceeded critical	The peg counts the number of times the critical Rfactor threshold was exceeded during the lifetime.

SIP Session

The following sections describe the SIP performance group data that can be viewed for a Oracle Communications Session Element Manager device.

SIP Session: Current Tab

Hostname	The hostname of the SIP session agent for which the following statistics are being calculated.
Index	A number for the sole purpose of indexing session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound current active sessions	The number of current active inbound sessions.
Inbound session rate	The current inbound session rate in the current performance session (CPS).
Outbound current active	The number of current active outbound sessions.
Outbound current session rate	The current outbound session rate in CPS.
Inbound admitted	Total number of inbound sessions during the period.
Inbound not admitted	Total number of inbound sessions rejected due to insufficient bandwidth.

Outbound admitted	Total number of outbound sessions during the period.
Outbound not admitted	Total number of outbound sessions rejected because of insufficient bandwidth.

SIP Session: Average period/state Tab

Hostname	The hostname of the session agent for which the following statistics are being calculated.
Index	The number for the sole purpose of indexing SIP session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound highest concurrent	The highest number of concurrent inbound sessions during the period.
Inbound average session rate	The average rate of inbound sessions during the period in current performance session (CPS).
Outbound highest concurrent	The highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered	The total number of answered sessions during the period.
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
Average one-way signaling latency (ms)	The average observed one-way signaling latency during the period.
Maximum one-way signaling latency (ms)	The maximum observed one-way signaling latency during the period.

CAC Tab

The following Call Admission Control (CAC) data is shown for the SIP session performance group:

Index	A number for the sole purpose of indexing SIP session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Current session utilization level	The call admission control (CAC) utilization value for sessions of SIP session agents.
Current burst rate utilization level	The CAC utilization value for burst rate utilization of SIP session agents.
Object ID	(Hidden) The SNMP object ID for the SIP session agent.

H.323 Session

H.323 Session: Current Tab

Hostname	The hostname of the session agent for which the statistics are being calculated.
Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound current active sessions	The number of current active inbound sessions.
Inbound session rate	The current Inbound Session rate in CPS.
Outbound current active	The number of current active outbound sessions.
Outbound current session rate	The current outbound session rate in CPS.
Inbound admitted	The total number of inbound sessions during the period.
Inbound not admitted	The total number of inbound sessions rejected due to insufficient bandwidth.

Outbound admitted	The total number of outbound sessions during the period.
Outbound not admitted	The total number of outbound sessions rejected because of insufficient bandwidth.

H.323 Session: Average Period/State Tab

Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Name	The hostname of the session agent for which the statistics are being calculated.
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound high current	The highest number of concurrent inbound sessions during the period.
Inbound average session rate	The average rate of inbound sessions during the period in CPS.
Outbound high current	Highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered	The total number of answered sessions during the period.
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90
Average latency	The average observed one-way signaling latency during the period.
Max latency	The maximum observed one-way signaling latency during the period.

NSEP

Use this performance group to view national security emergency preparedness (NSEP) data.

NSEP Pane

Current active sessions in	The number of current active inbound NSEP sessions.
Period high inbound	The highest number of concurrent inbound NSEP sessions during the period.
Total sessions in	The total number of inbound NSEP sessions during the period.
Period	The period for which the statistics are collected in seconds.
Current active sessions in	The number of current active NSEP sessions.
Total sessions in	The total number of inbound NSEP sessions during the period.
Period high in	The highest number of concurrent inbound NSEP sessions during the period.
Total not admitted	The total number of inbound NSEP sessions rejected.
Current active out	The number of current active outbound NSEP sessions.
Total sessions out	The total number of outbound NSEP sessions during the period.
Period high out	The highest number of concurrent outbound NSEP sessions during the period.
Total not admitted	The total number of outbound NSEP sessions rejected.

Trap Table Summary

Trap Table Summary Pane

Trap name	The trap name for this fault condition.
Number of variables	The number of variables encoded in the trap.
System uptime	The SNMP sysUptime when the trap was generated.

Storage Utilization

Storage Utilization Pane

Volume name	The name of the disk partition as defined by the user.
Total space (MB)	The total amount of disk space.

Available space (KB)	The free disk space that is available.

Intrusion Detection System (IDS)

IDS Performance Pane

SIP endpoint demotions from trusted to untrusted	The global counters for SIP endpoint demotions from trusted to untrusted.
SIP endpoint demotions from untrusted to denied	The global counters for SIP endpoint demotions from untrusted to denied.
MGCP endpoint demotions from trusted to untrusted	The global counter for MGCP endpoint demotions from trusted to untrusted.
MGCP endpoint demotions from untrusted to denied	The global counters for MGCP endpoint demotions from untrusted to denied.

Cached Contacts

Cached Contacts Pane

SIP local contacts	The number of active SIP local contacts.
MGCP GW endpoints	The number of MGCP GW endpoints.
H.323 registrations	The number of H.323 registrations.

Network Management Controls

NM Controls Pane

Name	The name of the network management (NM) control.
Type	The type of network management control.
Incoming total	The total number of incoming calls that match a destination identifier.
Rejected total	The total number of incoming calls that are rejected.
Diverted total	The total number of incoming calls that are diverted.
Incoming current	The number of incoming calls during the current period that match a destination identifier.
Rejected current	The number of incoming calls that are rejected during the current period.
Diverted current	The number of incoming calls diverted during the current period.

Incoming period max	The maximum number of incoming calls during a period that match a destination identifier.
Rejected period max	The number of the maximum incoming calls rejected in a period.
Diverted period max	The number of the maximum incoming calls diverted in a period.

ENUM Servers

ENUM Servers Pane

Config name	The name of the ENUM configuration.
Server IP address	The IP address for the ENUM server.
Server status	The status of the ENUM server.

View Codec and Transcoding Data

Codec data displayed by Oracle Communications Session Element Manager is available for supported C-series and D-Series Oracle Communications Border Controller (SBC) products.

> **Note:**
>
> SBCs need to have a transcoding NIU card for Codecs to work.

> **Note:**
>
> The TCU load stats unit for Codec Transcoding under Performance Manager is one of 10000th. For example, on the SBC CLI if the xcode load stats value is 0.16%, then on SDM UI the value for TCU load stats is 16.

Codec Statistics Pane

Realm name	The realm that corresponds with the listed codec.
Other	The codecs that are not matched with the standard, well-known list of codecs.

CPU Core Table

CPU Core Pane

Core index	A monotonic, increasing integer for the sole purpose of indexing.

Description	The core ID and slot location.
CPU usage	The percentage of total CPU being used.
State	The current CPU state.
Memory descriptor	The type of RAM memory.
Memory usage	The current amount of RAM being used by the CPU.

B

Session Element Manager Traps

A list of SNMP traps (SNMP Trap OIDs) that originate from devices that appear in OCSEM events and alarms.

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. In the **Select** dialog box, select the **AcmeSD** trap group row from the **Trap groups** table and click **OK**.
   The following list describes some of the SNMP traps that are supported by the product plugin.

Trap	Event Type	Description
apAcctMsgQueueFullClearTrap	**Account message queue**	The apAcctMsgQueueFullTrap condition was cleared.
apAcctMsgQueueFullTrap	**Account message queue**	The account message queue percentage threshold for being full was crossed.
apAclDropOverThresholdClearTrap	**ACL drop ratio below threshold**	The apAclDropOverThresholdTrap condition was cleared.
apAclDropOverThresholdTrap	**ACL drop ratio exceeded**	A number of ACL dropped connections has reached its threshold.
apAppsDnsServerStatusChangeTrap	**Application DNS server**	The reachability status of the Domain Name Server (DNS) server changed due to a communication subsystem failure due to a communication subsystem failure.
apAppsENUMServerStatusChangeTrap	**Enum server**	The reachability status of the ENUM server changed due to a communication subsystem failure.
apCoreLBMemberInServiceTrap	**Core Load Balancer**	A core load balance member becomes responsive after failure.
apCoreLBMemberOOSTrap	**Core Load Balancer**	A core load balance member is not responsive or out of service (OOS).
apDnsAlgConstraintStateChangeClearTrap	**DNS-ALG configuration constraint**	The DNS Application Layer Gateway (ALG) configuration object constraints state changes from Constraints Exceeded to In-Service.
apDnsAlgConstraintStateChangeTrap	**DNS-ALG configuration constraint**	The DNS-ALG configuration object constraints state changes from In-Service to Constraints Exceeded.

Trap	Event Type	Description
apDnsAlgStatusChangeClearTrap	**DNS-ALG server**	The reachability status of an DNS-ALG server changes from either Timed out or OOS to In-Service.
apDnsAlgStatusChangeTrap	**DNS-ALG server**	The reachability status of an DNS-ALG server changes from In-Service to either Timed out or OOS.
apEnvMonPortChangeNotification	**HotPlugHW**	For the AP4500 only. This trap occurs if a physical port is inserted or present, or removed or not present.
apEnvMonTempChangeNotification	**Temperature change**	The device crossed a temperature threshold.
apEnvMonVoltageChangeNotification	**Voltage change**	The device crossed a voltage threshold.
apH323StackMaxCallThresholdClearTrap	**H323 calls**	The number of H.323 calls decreases to below the lowest maximum call threshold.
apH323StackMaxCallThresholdTrap	**H323 calls**	The number of H.323 calls increases the percentage of the maximum calls threshold.
apLicenseNotApproachingCapacityNotification	**License**	The total number of active sessions on the system (across all protocols) has gone to or below 90% of its licensed capacity (but no sooner than 15 seconds after the original alarm was triggered).
apMonitorCollectorClearTrap	**SBC - CommMonitor connection**	Clears the communication monitor connection notifications.
apNNCReportingPswdExpiration	**Reporting**	The event warns that the Oracle database (OCSREMDW) user password and the BI Publisher database user passwords (DEV_MDS, DEV_BIPLATFORM, NNCENTRAL) that you configured in the Report Manager installation expire after 180 days. This warning appears 7 days before these passwords expire by default.
apNNCReportingPswdExpirationClear	**Reporting**	Clears the Oracle and BIPublisher database user password expiration warnings.
apSysMgmtGroupTrap	**apSysMgmt**	Associates with the proprietary Oracle ap-smgmt.mib. This specific trap provides a way to gather a grouping and gathering of system status information for CPU, memory, license, health, and so on.

Trap	Event Type	Description
apSysMgmtGroup trap	**ARP capacity**	Measures the ARP capacity, which is the percentage of the ARP table in content addressable memory (CAM) utilization.
authenticationFailure	**AuthTrap**	The standard authenticationFailure trap is used when the SNMPv2 agent received a protocol message that was not properly authenticated.
apSysMgmtGroupTrap	**CPU**	Measures the percentage of CPU utilization.
apSysMgmtAlgdCPULoadTrap	**CPU load**	Measures the percentage of CPU of application tasks has exceeded the threshold algd-load-limit
apSysMgmtDOSTrap	**DoS**	Displays the Oracle Denial of Service (DoS) protection proprietary trap.
apSysMgmtGatewayUnreachable	**Gateway**	This alarm displays the status of gateway reachability.
apSysMgmtExpDOSTrap	**Enhanced DoS**	Indicates a device exceeded configured thresholds and was denied access.
apSysMgmtFanTrap	**Fan**	Indicates that the fan unit speed fell below the monitoring level.
apSysMgmtH323InitFail	**H323 Stack**	Describes the status of H.323 stack.
apSysMgmtPushServerUnreachableTrap	**HDR**	This alarm indicates that the specified server becomes unreachable by the system collector.
apSysMgmtGroupTrap	**Health**	Indicates the system health percentages.
apLicenseApproachingCapacityNotification	**License**	Associates with the proprietary Oracle ap-license.mib, which provides information about the status of your system licenses.
linkDown	**Link**	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state.
linkUp	**Link**	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.

Trap	Event Type	Description
apSysMgmtMediaBandwidthTrap	**Media bandwidth**	This alarm indicates that bandwidth allocation failed at a percentage higher or equal to the system's default threshold rate.
apSysMgmtMediaPortsTrap	**Media ports**	This alarm indicates that port allocation failed at a percentage higher or equal to the system's default threshold rate.
apSysMgmtMediaUnknownRealm	**Media realm**	This alarm shows the status of the media realm.
apSysMgmtGroup	**Memory**	Displays the percentage of memory utilization.
apEnvMonStatusChangeNotification	**Monitor**	This alarm is associated with the proprietary Oracle ap-env-monitor.mib, which gathers information about fan speed, voltage, temperature, and power supply for the system. It also sends out traps when status changes occur.
apSysNATCapacity	**NAT capacity**	Shows the percentage of NAT table (in CAM) utilization.
apSysMgmtNTPClockSkewTrap	**NTP Clock Skew**	This alarm indicates NTP had to adjust the clock by more than 1000 seconds.
apSysMgmtNTPServerUnreachableTrap	**NTP server**	This alarm indicates that the specified NTP server is unreachable.
apSysMgmtNTPServiceDownTrap	**NTP service**	This alarm indicates that all configured NTP servers are unreachable.
apEnvMonStatusChangeNotification	**Power**	This alarm indicates the status of power supply.
apSysMgmtRealmMinutesExceedClearTrap	**Realm Minutes Exceeded**	This alarm describes the monthly minutes exceeded for a realm.
apSysMgmtRadiusDownTrap	**RADIUS Servers**	This alarm shows the status of the RADIUS server.
coldStart	**Reboot**	This alarm shows the proprietary version of the standard coldStart trap.
apSysMgmtRedundancyTrap	**Redundancy**	This alarm indicates that a state change occurred on either the primary or secondary system in a redundant (HA) pair.
apSysMgmtCfgSaveFailTrap	**Save-config**	Indicates that an error occurred while the system was trying to save the configuration to memory.
apSysMgmtStatusChange	**Session agent**	This alarm displays the session agent information, which includes the hostname, IP address, status, and the reason for the status.

Trap	Event Type	Description
apSysMgmtSingleUnitRedundancyTrap	**Single unit redundancy**	This alarm shows if the status of a slot changed. The varbinds contain the new information for the slot.
apSysMgmtSurrogateRegFailed	**Surrogate registration**	This alarm shows the status of surrogate registration and associated with the trap.
apSysMgmtTaskSuspendTrap	**Task**	This alarm indicates that there is a suspended task.
apSysMgmtTempTrap	**Temperature change**	Indicates the system temperature.
ColdStart	**ColdStart**	The SNMPv2 agent is reinitializing itself and its configuration may have been altered.
apSipRecRecDlgFailNotify	**SIP recording dialog failure**	This trap is generated when a Recording Dialog fails to send a timely response to a request, typically an in-dialog OPTIONS request.

Note:

The OCSDM does not process this trap if R2 26 compliance is enabled.