Oracle® Session Delivery Management Cloud

User's Guide

F30728-28
March 2026

Oracle Session Delivery Management Cloud User's Guide,

F30728-28

Contents

3 Device Manager

4 Security Manager

5 Configuration Manager

7 Work Order Manager

8 Route Manager

9 Administration

10 HDR Reports and Analytics

About This Guide

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) User Guide provides information about the administration and software configuration.

The following table describes the documentation set for this release.

Document Name	Document Description
Getting Started Guide	Contains conceptual and procedural information for system provisioning and software installations.
User Guide	Contains information about the administration and software configuration of the Oracle SDM Cloud.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective.
What's New	Contains a list of new features for a specific release as well as Known Issues pertaining to the release.

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	Description
July 2020	• Initial release.
September 2020	• Updates the following sections for accuracy: – Alarm and Event Configuration Tasks – Manage Transport Layer Security Certificates – Use an Offline Configuration for a Device Cluster – View and Save Audit Logs – Load the Configuration of a Local Device to Configure a Device • Removes the following unsupported sections: – Monitor SDM Server Health and Disk Usage – Use Oracle SDM Cloud to Configure Product Devices – Configure a Network Interface – Configure a Physical Interface • Adds the section "Configure a Configuration Element".
October 2020	• Updated for 20C October release.

Date	Description
December 2020	• Renames Chapter 1 from "Oracle SDM Cloud Dashboard Page Display and Operations" to "Dashboard Manager". • Updates all references of the Filter Portlets feature to the Filter feature. • Updates all references of the OMCE to MCE. • Renames "Adding Dashboards" to "Creating Dashboards". • Adds the section "Dashboard Editor". • Renames "Adding Portlets" to "Creating Portlets". • Updates the following sections for clarity and accuracy. – The Dashboard Header – Filter Component – The System Health Dashboard – Creating Dashboards – Creating Portlets – Oracle Communications Service Provider Edge and Core Plug-in Product Category and Network Function Types – Add a Mediation Engine Network Function with Devices – Load the Configuration of a Local Device to Configure a Device – Fault Manager – Customize Product Plugin Event Traps
January 2021	• Updated for 20C January 2021 release.
March 2021	• Fixes table formatting issue in "Manage Device Deployment Spreadsheets".
April 2021	• Updated for 20C April 2021 release.
July 2021	• Updated for 20C July 2021 release.
March 2022	• Updated for 20C March 2022 release.
July 2022	• Updated for 20C July 2022 release.
November 2022	• Updated for 22D November 2022 release.
February 2023	• Updated for 23A February 2023 release.
August 2023	• Updated for 23C August 2023 release.
November 2023	• Adds a note to "Dashboard Designer" regarding the number of custom dashboards supported.
December 2023	• Adds "Upload a NF Certificate" topic.
February 2024	• Updated for 24A February 2024 release.
August 2024	• Updated for 24C August 2024 release. • Adds a note to "Import a CSV File" regarding the need to create a Route Set.
November 2024	• Updated for 24D November 2024 release.
April 2025	• Updated for 25A April 2025 release.
October 2025	• Updated for 25D October 2025 release.

1

Dashboard Manager

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Dashboard displays information about configured devices and provides tools to help you view devices and fault management statistics.

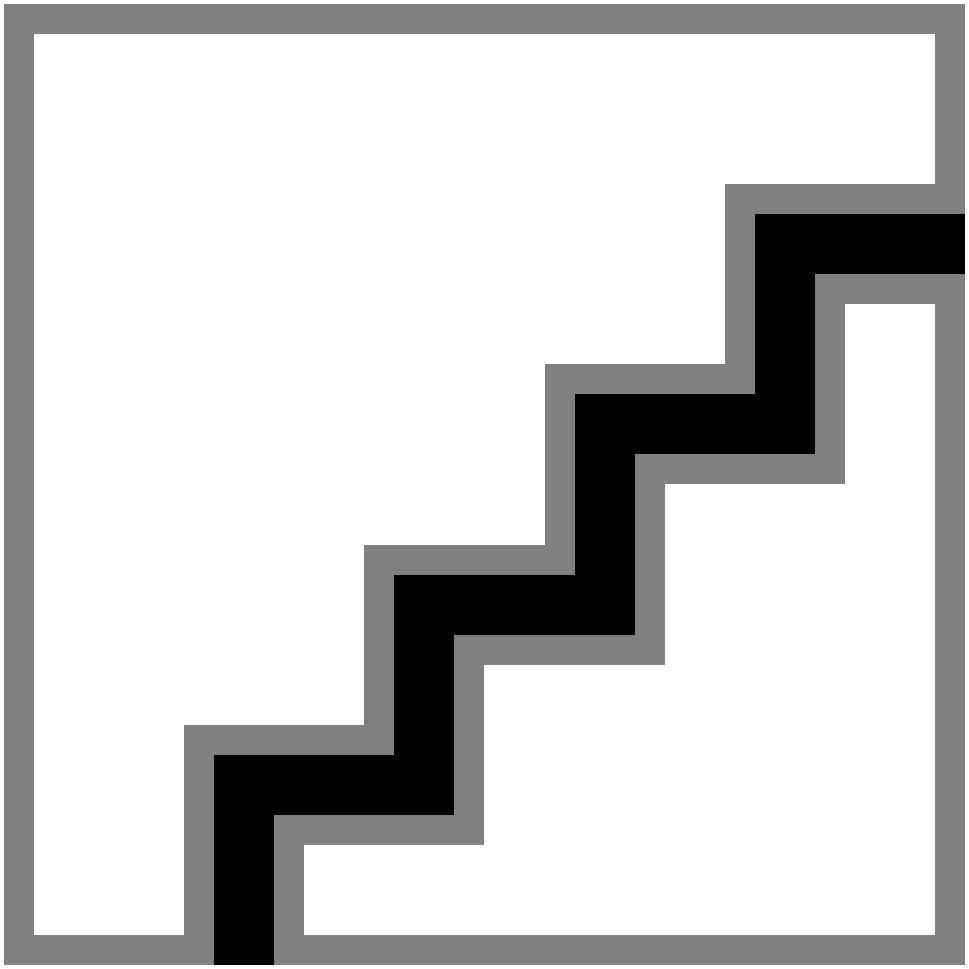
> **Note**
>
> A device is any entity managed by the Oracle SDM Cloud and represents a network element.

Upon initial login, the Oracle SDM Cloud sets the System Health Dashboard as the default dashboard if a default dashboard has not been selected for the logged in user. The System Health Dashboard contains 14 preexisting portlets that display the aggregated data over all the devices added in the Configuration Manager. A portlet is a self-contained component on the Dashboard that presents information in textual or graphical format.

While the Oracle SDM Cloud comes with one preexisting System Health Dashboard, via the Dashboard Manager, users can either create customized portlets or use the existing portlets to create customized dashboards.

The Dashboard Header

After you log on, using the credentials you received with your subscription, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) service displays the System Health Dashboard as the default landing page. At the top of the page, the Oracle header displays the username of the user signed in and their User Group, provides access to the User menu, and displays the Tools tab.

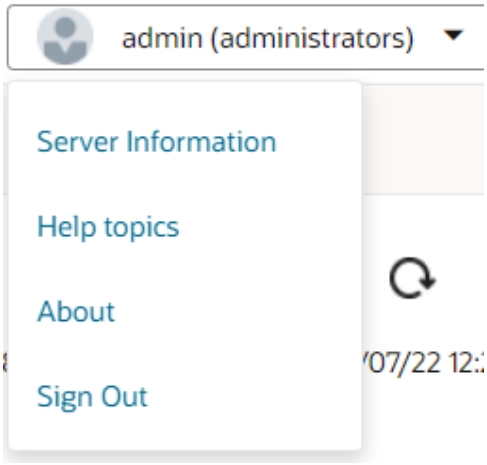


The User Menu—Displays when you click the user name. The User Menu provides additional user options such as Switch Roles, Help Topics, About, and Sign Out.

The Tools Tab—Provides additional tools. Currently, certificate management is the only tool offered.

The User Menu

In the upper right hand corner of the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) landing page, Oracle SDM Cloud displays the username of the user who is logged in, as well as their User Group. When you click the address, the GUI displays the user menu.



Server Information—Displays the server name.

Help topics—Provides a link to the Oracle Communications help center.

About—Displays information about the Oracle SDM Cloud including Version, Release Number, and Product name.

Sign Out—Displays the **Sign Out** control that you use to log off from the Dashboard.

The Dashboard Page

While the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) displays the System Health Dashboard upon initial login, you have the ability to design and build custom portlets and dashboards, saving multiple copies, set default dashboard, and the option to make a dashboard shared, public, remain private, or remain in draft state. A portlet is a self-contained component on the Dashboard that presents information in textual or graphical format.

By default, the Oracle SDM Cloud displays data over the past 24 hours aggregated over all managed devices. However, you can also customize the data for a particular time frame by clicking the Filter icon in the upper righthand corner of the page.

The dashboard also contains the **AutoRefresh** icon, allowing users to set a time interval, in seconds, at which the Oracle SDM Cloud refreshes all data within each portlet on the dashboard. The minimum allowable value is **15** seconds (the default) and the maximum is **3600** seconds.

In addition to the **Filter** and **AutoRefresh** icons, there is the **Refresh** icon to refresh the statistics and an **Information** icon which provides a brief description of the Dashboard.

Filter Component

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides data content filtering capabilities Dashboards and Portlets. The Filter icon provides specific criteria upon which the end user can filter data content. The Filter appears on the following pages:

- Dashboard Manager
- Dashboard Editor
- Portlet Editor

From the **Dashboard Manager** page, the **Filter** icon allows you to filter the data content that each Portlet renders, in the default Dashboard that is currently active.

The following fields appear in the Filter dialog box:

- **Time Increment**
- **Start Time**
- **End Time**
- **Select Device**

The following table describes the Filter Fields:

Filter Criteria	Description
Time Increment	Indicates the frequency of data aggregation The following are available options: • Raw—Every 5 minutes • HR (default)—Every hour • Daily—Every day • Weekly—Every week • Monthly—Every month
Start Time - **End Time**	Indicates the interval to be used to fetch data based on the selected time increment. The default setting is the last 24 hours from the current date and time. Click the calendar icon to select start and end days from the calendar. These times are presented based on the browser's local time zone.
Start Time (UTC) and **End Time (UTC)**	These are read-only fields that display the selected time. For consistency, all date and time sensitive data sets are stored and rendered in UTC. These fields provide the required mapping in UTC. • Raw—The last 2 hours • HR (default)—The last 7 days • Daily—The last 14 days • Weekly—The last 28 days • Monthly—The last 365 days
Select Device	Allows you to select the Devices or Device Groups for this portlet. The devices from which you select are devices which have been added to Configuration Manager and are the correct device product type based on the monitoring data source. By default, if no devices are selected, the portlet displays data for all devices on the Oracle SDM Cloud (except when accessed from the **Add Portlet** screen). For more information on selecting a device via the Filter dialog, see "Adding Portlets".

The System Health Dashboard

The System Health Dashboard displays upon initial login. The Dashboard contains 14 preexisting portlets which report in Coordinated Universal Time (UTC).

The following portlets display in the System Health Dashboard:

- Average Concurrent Sessions—The average number of concurrent sessions across the devices.
- Sites—The number of sites associated with this Oracle SDM Cloud.
- Device Types—A percentage of device types on this Oracle SDM Cloud.
- Device Status—The number of reachable Management Cloud Engines (MCEs), compared to the number of configured MCEs, as well as the number of reachable devices to the total number of devices in the Device Manager.
- Transactions Per Second—The maximum of average transactions measured over the last 24 hours as well as the total TPS purchased by the user.

  > **Note**
  >
  > This value provides important input to determine if you are close to exceeding your license limit. For more information, contact your Oracle representative.

- DB Usage Status—The percentage of total database capacity used by devices to which the user has access.

  > **Note**
  >
  > This value provides important input to determine if you are close to exceeding your license limit. For more information, contact your Oracle representative.

- Alarms—The number of Critical, Emergency, Major, and Minor Alarms. By default, users are able to see system level and device level data for devices to which they have access. By clicking on an alarm severity, users can navigate directly from this portlet to the Alarms page. For more information, see *Navigate Directly From Connectivity Status and Alarm Portlets*.
- CPU—Average CPU utilization of the selected devices.
- Memory—Average memory utilization of selected devices over the selected time increment.
- Concurrent Sessions—The total number of transactions within the specified period of time.
- Health—An overall measure of the health of the devices, aggregated over time and devices.
- Connectivity Status—The average reachability and unreachability of all the devices for the selected time increment. By clicking on Reachable or Unreachable, users can navigate directly from this portlet to the Devices page with the appropriate filter. For more information, see *Navigate Directly From Connectivity Status and Alarm Portlets*.
- Average Registered Users—The average number of registered users across the devices.
- Average Active Calls—The average number of active calls across the devices.

> **Note**
>
> Users are able to view portlet data only for the devices they have access to per Security Manager User Group Permissions. However, system level portlets such as Sites, Device Types, Management Status, Device Status, Transactions per second, and DB usage continue to show system level information including all MCEs, sites, and devices.
> For more information, see "Apply or Change User Group Privileges" in the Security chapter.

Navigate Directly From Connectivity Status and Alarm Portlets

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows users to navigate directly from the Connectivity Status and Alarms Portlets to related pages, such as Device Manager and Alarms Pages.

This feature enables users to view filtered results by selecting a connectivity status or an alarm severity, enhancing usability by providing click-based navigation and pre-filtered search results.

To navigate from the **Connectivity Status** portlet, click on **Reachable** or **Unreachable**. Alternatively, hover over and click a bar in the graph within the portlet specifying a time. The **Device Manager**, **Devices** page displays showing all of the devices with the connectivity status or time you selected. When you click the **Search** button on the **Devices** page, the **Connectivity Status** field automatically displays pre-filled values.

Navigation works consistently when the portlet is zoomed in.

> **Note**
>
> If a Management Cloud Engine (MCE) becomes unreachable and lacks a backup, all associated devices are marked as unreachable.

To navigate from the **Alarms** portlet, click on the severity level to filter on; either **Critical**, Emergency, **Major**, or **Minor**. Alternatively, hover over and click a bar in the graph within the portlet specifying a severity. The **Alarms** page displays showing all of the alarms with the severity that you selected. When you click the **Search** button on the **Alarms** page, the **Severity** field automatically displays pre-filled values.

Navigation works consistently when the portlet is zoomed in.

The Dashboard Slider Menu

By clicking the Expand icon in the upper left hand corner of the Dashboard, you can view the Dashboard's slider menu.

The slider menu allows you to access, view, and manage the Oracle SDM Cloud's dashboards, devices, security, configuration, fault, work orders, route manager, and Administrations.

Dashboard Designer

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows you to design and build custom dashboards using the Dashboard Manager.

Access the Dashboard Designer under the **Dashboard Manager**. The Dashboard Designer displays a list of all previously created dashboards and it is from here you are able to navigate to the Dashboard Editor. The dashboards in this list can fall under one of the following categories.

> **Note**
>
> The Oracle SDM Cloud can support up to 100 custom dashboards.

Mode	Owner's Permissions	Other Users' Permissions	Description
Draft	• View • Copy • Edit • Delete	N/A	The author has created a draft of the dashboard and no other users have access to it until the author publishes it as Shared or Public. It appears in the author's dashboard list only.
Private	• View • Copy • Edit • Delete	N/A	The author is publishing the dashboard in private mode and no other users have access to it. It appears in the author's dashboard list only.
Shared	• View • Copy • Edit • Delete	• View • Copy	The author is publishing the dashboard to be viewed by other users, however, other users cannot edit or delete. It appears in all users' dashboard lists.
Public	• View • Copy • Edit • Delete	• View • Copy • Edit • Delete	The author is publishing the dashboard publicly, granting all other users full permissions. It appears in all users' dashboard lists.

The dashboard list includes the predefined System Health Dashboards. This predefined dashboard is available to copy and set as default only and cannot be edited or deleted.

At the top of the Dashboard Designer screen you can select from 2 views:

- **All**—Displays the total number of dashboards saved on the Oracle SDM Cloud including private and draft state of the logged in user only, public, shared, and pre-defined dashboards.
- **Favorite**—Displays the total number of dashboards you have marked as a Favorite.

The Dashboard Designer List View displays the following buttons and fields:

- **Search** field—The search functionality pre-populates as you enter the Dashboard name, listing dashboards starting with the characters entered. The search field also supports wild card searches (*). The search field lists dashoards based on the view selected.
- **Refresh** button—Refreshes the Dashboard list.
- **+Dashboard** button—Create a new dashboard.
- **Set Default** button—Set the dashboard as the default dashboard.
  Select an entry in the dashboard list table and click **Set Default** to set the selected dashboard as the default dashboard for that user only. A user can only set a dashboard as default when it is in either the private, public, or shared state and can only make a private dashboard a default if it is their own. Dashboards in the draft state cannot be set as default.
- **Set Columns** button—Launches the Set Columns pop-up, allowin gyou to select which columns appear in the table.
  The following lists the Dashboard table columns:
  - **Dashboard** column header—Specifies the number of portlets present on that dashboard.
  - **Name** column header—The name of the dashboard. This name must be unique.
  - **Description** column header—Description of the dashboard.
  - **State** column header—Specifies the state of the dashboard, either Draft, Private, Shared, or Public.
  - **Favorite** button—Select the heart icon to mark as a Favorite dashboard.
  - **Delete** button—Delete the dashboard.
  - **Edit** button—Edit the dashboard. Clicking this button brings you to the Dashboard Editor page.
  - **Copy** button—Create a copy of the dashboard in draft state. This copy is added to the dashboard list.

Dashboard Editor

The Dashboard Editor is where you can create new dashboards or modify existing dashboards. The Editor allows you to select which portlets to add and remove to or from a dashboard, and lets you position them as you want within the dashboard.

Creating Dashboards

From the Dashboard Designer page you can navigate to the Dashboard Editor page and create a new dashboard by selecting and adding portlets. You can select up to twenty portlets, from different device types, to create a new dashboard.

When you create a new dashboard the default filters to render a graph are automatically applied until you set filter criteria for that dashboard using the **Filter** icon. Once you set this criteria, these filters are applied to any portlets you add to this dashboard going forward. For more information on using the **Filter** icon, see "Filter Component".

To create a new dashboard:

1. Navigate to **Dashboard Manager**, **Dashboard Designer** and click the **+ Dashboard** button to bring up the Dashboard Editor.
2. **Dashboard Title**—Click the pencil icon to enter a unique name for this dashboard.

3. **Dashboard Description**—Click the **Dashboard Description** icon. The Dashboard Description dialog appears. Enter a brief description of this dashboard and click **OK** to save the description or **Cancel** to discard the changes and exit out of the dialog.
4. **Add Portlet**—Click the **Add Portlet** icon to open the Select Portlet to Dashboard dialog box.

> **Note**
>
> Twenty is the maximum number of portlets allowed per dashboard. If you try adding more than twenty portlets, the Oracle SDM Cloud displays an error message.

The Select Portlet to Dashboard lists all of the portlets available to use. The portlets included in this list include the following:

- Private (Only this user's Private portlets display)
- Shared
- Public
  Shared and Public portlets can be added to an author's private and shared dashboards and to any public dashboards. However, Private portlets can only be added to Private and Draft dashboards. Dashboards cannot be made Shared or Public if they contain one or more private portlets. The Oracle SDM Cloud displays a warning message and prevents a user from changing the state of a dashboard with a private portlet. For more information on the types of portlets, see "Creating Portlets".
  - **PREVIEW**—View a preview of this portlet's data. This shows the data available from the database until the next polling cycle. Note that you cannot preview the existing portlets that come with the Oracle SDM Cloud, only portlets created by a user.
  - Select the checkmark for the portlet to add to the dashboard. You can add more than one portlet at a time. The maximum number of portlets allowed to be added to a dashboard is 20.
  - Add all of the portlets you want to add. Close the dialog box by either clicking **Done** to save your changes or clicking the X to cancel the changes made.

  You are returned to the Dashboard Editor page. The dashboard is updated with the newly added portlets.

  Use the Drag Handle icon located on each portlet to drag and drop the portlet to change the portlet order within the dashboard.
5. **Cancel** button—Cancels the edit operation and returns you to the Dashboard Designer page.
6. **Save Draft** button—Saves the dashboard as a draft. To be saved, you must have provided a dashboard name. Once a dashboard is published as public, private or shared, it cannot return to draft state and the **Save as Draft** button is disabled.
7. **Publish** button—Publishes the dashboard. Select the mode in which you want the dashboard to be published:
   - Private
   - Shared
   - Public

For more information on the supported dashboard modes, see "Designing Custom Dashboards".

Once you select **Publish**, you are returned to the dashboard list screen and the new dashboard appears in the list.

8. **+**—The Add Portlet button is another way to select a portlet to add to this dashboard.
9. **Dashboard Filter** icon—The Dashboard Filter icon allows you to filter the data content rendered by each portlet in the dashboard based on **Time Increment**, **Start Time** and **End Time**, and **Device**.
10. **Refresh** icon—Refreshes portlet data displayed on the dashboard with the selected filter criteria.

Edit a Dashboard

With the appropriate permissions, you can edit dashboards (those that are in an editable state) via the Dashboard Editor page.

When editing existing dashboards, the following rules apply regarding the state of the dashboard:

- **Draft**—When you edit a dashboard that is in the draft state, both the **Save Draft** and **Publish** buttons are enabled.
- **Private**—When you edit a dashboard that is in the published but private state, the **Save Draft** button is disabled. Once a dashboard has been published, it cannot be reverted back to the draft state. Publish as either **Private**, **Shared**, or **Public** to save your changes.
- **Shared**—When you edit a dashboard that has been published as shared, the **Save Draft** and **Private** buttons are disabled. Once a dashboard has been published as shared, it cannot be made private again. Publish as either **Shared** or **Public** to save your changes.
- **Public**—When you edit a dashboard that has been published as public, the **Save Draft**, **Private**, and **Shared** buttons are disabled. Once a dashboard has been published as public it cannot be reverted. Publish as **Public** to save your changes.

To edit a Dashboard:

1. Navigate to the **Dashboard Designer** page.
2. Select the dashboard to edit and click the pencil icon.
   The Dashboard Editor page displays.
3. Update the dashboard as necessary.

> **Note**
>
> The **Dashboard Title** is read-only and cannot be modified on the Dashboard Designer page.

4. Save your changes by either clicking **Publish** or **Save as Draft**. To discard your changes, click **Cancel**.
   You are returned to the Dashboard list.

Dashboard Portlet Settings

When you are in the process of either creating or editing a dashboard, you can update some settings for the portlets within.

The portlets contain the following buttons:

- **Drag Handle** icon—Clicking this button you can drag and drop the portlet and change the portlet's order within the dashboard.

> **Note**
>
> The Oracle SDM Cloud also allows you to right-click with the options to **Cut**, **Paste Before**, and **Paste After**.

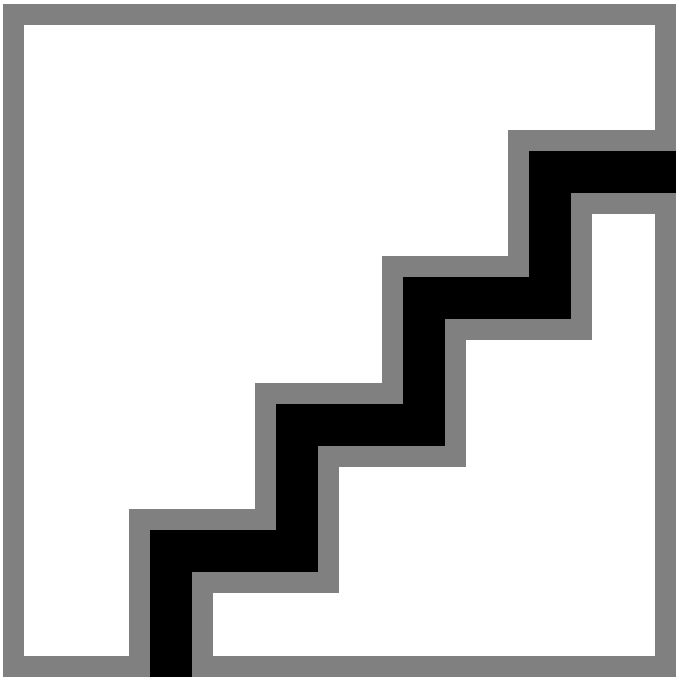
- **X** icon—Remove this portlet entry from the dashboard.

Customize the Display

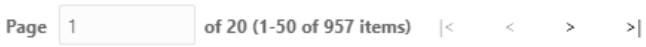
Depending on the features that you use in the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), you can change the way information is displayed in some of the tables, by selecting which columns appear in the table, customizing the way columns are displayed, and customizing how entries in a table are ordered. You can also customize the number of records that are displayed per page.

To customize the columns in a table:

1. From a table within the Oracle SDM Cloud, click **Set Columns**.



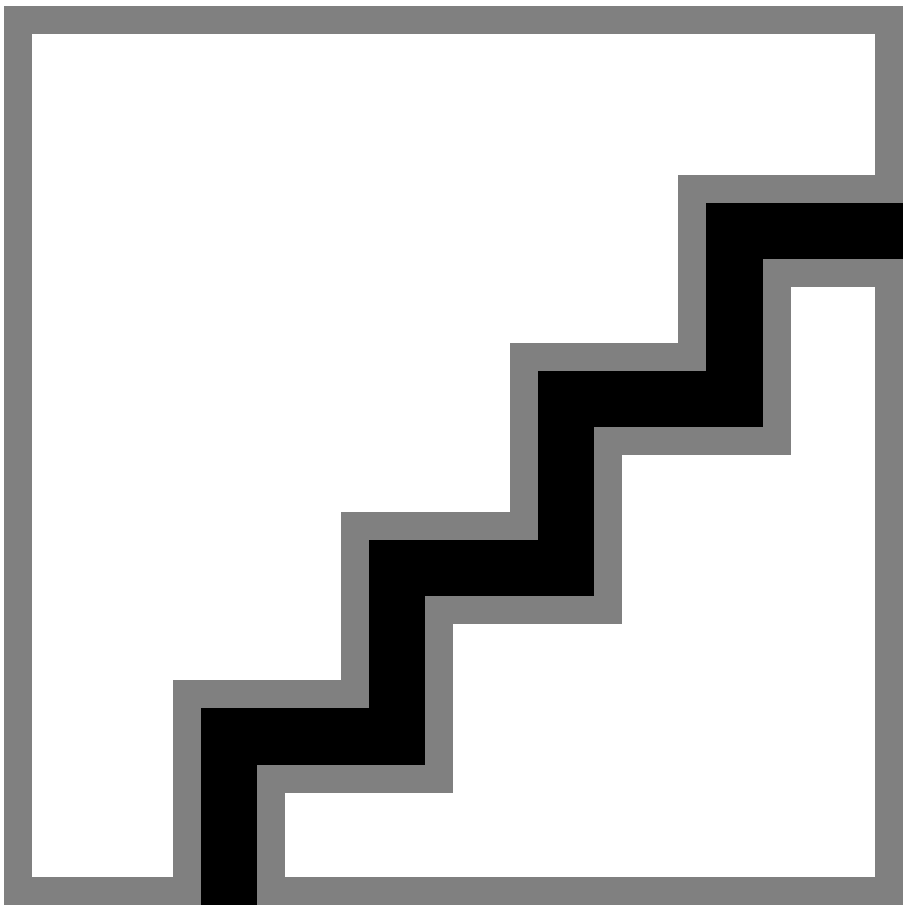
2. Select the columns you want to appear in the table.
3. Click **OK** to save and implement the changes or Reset to cancel and close the Set Columns popup.
4. Click a column header to sort the table entries by either ascending or descending order.
5. To display a page of records that you want to view, use the buttons at the bottom of the table to move between pages, or enter the page number you want.



6. To customize the number of records that are displayed per page, click the **Page Size** arrows up or down.

Get Help Tips for Fields and Menus

You can find various help tips for fields and menus that appear in the GUI by clicking on a field or attribute name to make a help tip appear. For example:



Designing Custom Portlets

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows you to build custom portlets that you can then use to design customized dashboards using the Dashboard Manager's Portlet Designer.

The Portlet Designer provides the following features:

- A list of existing portlets published and ready for use. These preexisting Oracle SDM Cloud portlets are used to power both preexisting Oracle SDM Cloud dashboards and can be used to build customized dashboards. As these dashboards are used in preexisting Oracle SDM Cloud dashboards, they cannot be modified, copied, or deleted. When you create your own customized portlets you have full management of the portlet's life-cycle. There are 6 preexisting data sources:
  - Average Calls Per Second
  - Average Concurrent Sessions
  - Average CPU Utilization
  - Average Health Score
  - Average Memory Utilization
  - Connectivity Status
- A Portlet Editor that allows you to create, view, copy, or edit portlets, as well as the following features:
  - A Monitoring Data Source Table to display and select from the exiting Data Source. A Data Source can represent KPI scalar to tabular value as well as network metrics that Oracle SDM Cloud solution provides.
  - The ability to create and configure a new monitoring Data Source, modify an existing data source configuration, or delete a monitoring data source.
  - A viewer where the portlet graphical representation can be viewed as the user is designing the portlet.
  - A graphical selector which allows you to select the needed graph type.
  - The ability to save a draft of a portlet that is being worked on or publish the final portlet for private, public, or shared usage.
  - Filter capabilities to focus on specific data content when building a portlet.

Access the Portlet Designer under the **Dashboard Manager**. The Portlet Designer displays a list of all previously created portlets, including the Oracle SDM Cloud preexisting portlets, as well as portlets created by the user and other users' shared and public portlets.

At the top of the Portlet Designer screen you can choose from the following 3 views:

- **All**—Lists all portlets saved on the Oracle SDM Cloud. This includes drafts created by the logged in user, portlets published as private for the logged in user, and all shared (view-only) and public portlets.
- **Favorite**—Lists the portlets you have marked as a Favorite.
- **In Use**—Lists the portlets currently used in Dashboards.

The Portlet Designer List View displays the following buttons and fields:

- **Search** text box—The search functionality pre-populates as you enter the Portlet name, listing portlets starting with the characters entered. The search field also supports wild card searches (*). The search field lists dashboards based on the view selected.
- **+ Portlet** button—This button launches the Portlet Editor where the user can create a new Portlet and add it to the list of Portlets.
- **Set Columns** button—Launches the **Set Columns** pop-up, allowing you to select which columns appear in the table.
  The following lists the Portlet table columns:

- **Portlet**—A thumb nail representation of the graph type the portlet is based on is presented. By clicking on this thumb nail, a preview of the portlet, displaying real data polled from the managed Network Functions, appears on the screen.
- **Name**—Name of the portlet.
- **Description**—Description of the portlet.
- **State**—(Hidden) The state of the portlet. This can be either **Draft**, **Private**, **Shared**, or **Public**.
- **Favorite**—Select heart icon to mark as a Favorite portlet.
- **Delete**—Delete the portlet.
- **Edit**—Edit the portlet.
- **Preview**—Preview the portlet. The portlet displays with real data from the last polling from the product type, data source, and default filter.
- **Copy**—Create a copy of the portlet. This copy is added to the portlet list.

> **Note**
>
> The preexisting portlets provided by the Oracle SDM Cloud do not allow certain actions to be performed, such as Delete, Edit, Preview, or Copy. In these cases, the options will be disabled.

- **Refresh** icon—Refreshes the Portlet list.

Creating Portlets

From the Portlet Designer page, you can navigate to the Portlet Editor page and create a new portlet. The Portlet Editor page contains the Monitoring table. This table contains all of the Data Sources currently created and saved on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud). You can either use existing Data Sources to create a portlet, or you can create new Data Sources using the Data Source Wizard. For more information on using the Data Source Wizard to create new Data Sources, see "Creating a New Data Source".

In addition to selecting Data Sources, you also select the graph type in which the Oracle SDM Cloud displays the data. The following graph types are supported:

- Multi-metric line time series
- Multi-metric bar time series

Prior to plotting a graph for a portlet, you must select a device for this portlet to filter via the Filter icon and then a data-source. The **Portlet Editor Filter** icon, once selected, provides a set of values which the end user can filter as follows:

- Time increment—Oracle SDM Cloud provides different spacial aggregated time increments for viewing.
- Start and End time—Select the start and end times for data retrieval if the data is time series based.
- Start Time (UTC) and End Time (UTC)—(read-only) Displays the user selected start and end times in UTC.
- Select Device—Target one or more devices. This can be selected from a device selection table, which provides the ability to search on each column.

If you plot a graph for a portlet before you have selected a device, when you click Preview, the Oracle SDM Cloud displays the message, "At least one Device and Data Source need to be selected to create this graph".

For Device Groups, the Oracle SDM Cloud displays the parent of the Network Function device. For Device, it displays devices based on the Device Group selection.

Once you select a device for your portlet, the Monitoring table is filtered based on the products being associated with those specific devices.

To create a new portlet:

1. Navigate to **Dashboard Manager**, **Portlet Designer** and click the **+Portlet** button to bring up the Portlet Editor.
2. Click the **Filter** icon.
   The Filter dialog appears.
3. **Select Device**—Click **Select Device** to bring up the Select Device table.
4. Select the Device Group or Device you require to filter the data set on that will be used to help visualize this portlet.

   > **Note**
   >
   > The Oracle SDM Cloud provides a grid paged table to easily navigate to different device groups and devices. In addition, the table provides character-based filter options on each column to quickly filter to specific devices of interest.

5. Click **Apply**.
   The **Devices +** count appears at the top of the Portlet Editor screen. When devices have been selected and applied, the button label changes from **Devices** to **Devices +n**. When you click on that button, it displays a breakdown of the devices as the following example shows:

   ```
   Number of Selected Devices: 5
   SBC: +3; ME: +2
   ```

6. Click the **Graph Type** icon. The Select Graph Type dialog appears. The Oracle SDM Cloud supports the following graph types:
   - Multi-metric time series line graph (default)
   - Multi-metric time series bar graph
7. ***Portlet Title** icon—Click the pencil icon to enter a unique name for this portlet. This is a required field and if you do not provide a Portlet Title, the Oracle SDM Cloud cannot save a draft or publish this portlet.
8. **Portlet Description** icon—Click the **Enter Description** icon next to **Portlet Title**. The Portlet Description dialog appears. Enter a brief description of this portlet and click **OK** to save the description or **Cancel** to discard the changes and exit out of the dialog.
   The **Monitor** table provides a list of existing Data Sources. Click the **Select** checkbox to select a Data Source for the portlet or create a new Data Source.
9. **+ Data Source**—Create your own Data Source. This button launches the Add Data Source Wizard. For more information on adding data sources and using the Data Source Wizard, see "Creating a New Data Source".
   Once you select a Data Source type from the Monitor table, the Portlet Editor displays a preview of the graph.

10. Click One of the following:
    - **Cancel**—When you click the **Cancel** button the Oracle SDM Cloud displays a confirmation message asking to press **Yes** to continue and discard changes or **No** to return to the previous screen.
    - **Safe Draft**—Saves a draft of the edits made, but the portlet cannot be used in a Dashboard until it is Published.
    - **Publish**—Presents a drop-down list with the following publishing options.
        - Private—This is a published portlet that can only be viewed by the author.
        - Shared—The portlet is published, viewable, and can be copied by other users so that they can create their own new portlet based on the shared portlet.
        - Public—The portlet is available to all users to edit, preview, copy, or add to dashboards.

Creating a New Monitoring Data Source

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows you to create a new data source, called a Monitoring Data Source (MDS), to be used in a portlet, defining the characteristics and adding it to the Monitoring table. A MDS is a common construct of how a NF-specific Key Performance Indicator (KPI) or metric is present to the end user. Oracle SDM Cloud provides the Add Data Source wizard to create new MDSs. All MDSs that are created are displayed in the Monitoring table.

The Add Data Source Wizard has 3 steps:

- **Data Source**—This page walks you through the steps to define a MDS construct that will be added to the Monitoring table (and, if required, added to the Poller metric table to enable polling for the metric).
- **Aggregation**—For Oracle SDM Cloud purposes, aggregation means the collection of sampling metrics into statistical clusters such as average, sum, count, minimum, and maximum statistics. There is no comparison or correlation in these statistic representations. The Oracle SDM Cloud allows you to configure the way you want to view the aggregated data.
  There are two types of aggregation that the Oracle SDM Cloud provides for you to select the required statistics. These types are:
    - **Spatial Aggregation**—When Oracle SDM Cloud samples for specific historical time series based KPI and metrics, the data samples periodically from the devices is called Raw data. As the data is being collected, Oracle SDM Cloud further aggregates the Raw data and provides statistics for hourly, daily, weekly, and monthly time increments. This type of aggregation over a time series is called Spatial Aggregation.
    - **Device Aggregation**—The collection of sampling metrics over individual Network Functions (NFs), or devices. When applying the Filter in dashboards or designers, the device selection will filter data sets specific to the selected devices. If more than one device is selected, Oracle SDM Cloud applies another aggregation over the values returned by each device. These generated statistics are called Device aggregation. For example, average, sum, count, minimum, or maximum statistics calculated over one or many devices.
- **Device Product**—The type of product from the session delivery portfolio, so that the data shows only for those products (for example, SBC, SR, or ME). Based on the **Data Source** selected, the list of products is filtered to only those products that support that metric.

To add a new data source:

1. From the Portlet Editor page, click the **+ Data Source** button.
   The Add Data Source wizard launches.
2. **Data Source**
   - **Data Source Display Name**—Enter a unique Data Source Display Name to use for this new data source.
   - Select the data source you want or search for a particular data source.
     When you click on a Data Source, information about that Data Source displays on the left of the screen, including Category and Data Source Type.

     > **Note**
     >
     > The Data Source Type currently supported by Oracle SDM Cloud are displayed here by the wizard. These data source types are supported by at least one or more products such as SBC, E-SBC, SR, or OCSM (Mediation Engine).

   - Click **Next**.
     The Aggregation screen displays.
3. **Aggregation**
   - **Select Spacial Statistic**—Select the aggregation type to use for spacial statistics.
   - **Select Device Aggregation**—Select the aggregation type to use for device aggregation.
   - Click **Next**.
     The Device Product screen displays.
4. **Device Product**
   - **Select Device Product Type**—Select the product type that you want the Monitoring Data Source to display data sets for.
   - Click **Finish**.
     The new Monitoring Data Source just created appears in the Monitor table.

Edit a Monitoring Data Source

Once you have created a Monitoring Data Source (MDS), you can edit the Device Product only. The Data Source type and Aggregation cannot be changed.

To edit a Monitoring Data Source:

1. Navigate to the **Portlet Editor** page.
2. In the Monitor table, click the **Edit** icon next to the Monitoring Data Source you want to edit.
3. Update the **Device Product** page as necessary.
4. Click **Finish**.

> **Note**
>
> Users can edit only the Data Sources that they have created.

Edit a Portlet

With the appropriate permissions, you can edit portlets (those in an editable state) via the Portlet Editor page.

When editing existing portlets, the following rules apply regarding the state of the dashboard:

- **Draft**—When you edit a portlet that is in the draft state, both the **Save Draft** and **Publish** buttons are enabled.
- **Private**—When you edit a portlet that is in the published but private state, the **Save Draft** button is disabled. Once a dashboard has been published, it cannot be reverted back to the draft state. Publish as either **Private**, **Shared**, or **Public** to save your changes.
- **Shared**—When you edit a portlet that has been published as shared, the **Save Draft** and **Private** buttons are disabled. Once a dashboard has been published as shared, it cannot be made private again. Publish as either **Shared** or **Public** to save your changes.
- **Public**—When you edit a portlet that has been published as public, the **Save Draft**, **Private**, and **Shared** buttons are disabled. Once a dashboard has been published as public it cannot be reverted. Publish as **Public** to save your changes.

To edit a Portlet:

1. Navigate to the **Portlet Designer** page.
2. Select the portlet to edit and click the pencil icon.
   The Portlet Editor page displays.
3. Update the portlet as necessary.

> **Note**
>
> The Portlet Title is read-only and cannot be modified on the Portlet Designer page.

Delete a Monitoring Data Source

To delete a Monitoring Data Source (MDS):

1. Navigate to the Portlet Editor page.
2. In the Monitor table, click the **Delete** icon next to the MDS you want to delete.
   A Confirm dialog appears asking you to confirm you want to delete that MDS.
3. Click **Yes** to proceed or **No** to cancel.

> **Note**
>
> Users can delete only the Data Sources that they have created.

2

Monitoring Manager

The **Monitoring Manager** provides a set of tools that allow the user to monitor the Oracle Communications Session Monitor (OCSM).

The **Monitoring Manager** slider allows you to do the following:

- Render the Recent Calls table on demand, displaying information about the 50 most recent calls. The Recent Calls table displays fresh data, differing from KPIs, which are maintained as historical data.
- Provides on-demand ladder diagrams for each call in the Recent Calls table. Within the ladder call diagrams, the user can choose which information to display and then export the ladder diagrams.
- Manage Mediation Engine (ME) Recent Call Access permissions for users with ME Recent Call Access **User Management** permissions.

Manage Mediation Engine Recent Calls

When the user adds an Oracle Communications Session Monitor (Session Monitor) to the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), the Oracle SDM Cloud polls the Session Monitor regularly and displays the Recent Calls on the Oracle SDM Cloud's **Monitoring Manager**, **Calls** page. For more information on adding an Session Monitor as a device, see "Add a Mediation Engine Network Function with Devices".

The Oracle SDM Cloud communicates with the Session Monitor using REST and, therefore, must generate the REST API key within the Session Monitor Admin page. For more information on using the Session Monitor and generating a REST API key, see https://docs.oracle.com/en/industries/communications/session-monitor/index.html.

Once the Oracle SDM Cloud and Session Monitor are properly authenticated, the Oracle SDM Cloud provides on demand recent call data. New data is fetched either when you navigate to the Recent Calls page or when clicking the Refresh button. The Oracle SDM Cloud retrieves and displays up to 50 recent calls per ME added as a device.

The Recent Calls page contains the following buttons and fields:

- **Filters** button—Allows you to filter the Recent Calls table. For more information, see "Filter Recent Calls".
- **Clear** button—Clears all currently applied filters.
- **Ladder Diagram** icon—Select a call in the table and click the Ladder Diagram icon to display a ladder diagram of the call. For more information on viewing ladder diagrams, see "View, Export, and Download Call Ladder Diagrams".
- **Download Message Flow** icon—Select a call in the table and click the Download Message Flow icon to download a ladder diagram of the call. For more information on downloading ladder diagrams, see "View, Export, and Download Call Ladder Diagrams".
- **Search** icon—Displays the **Recent Calls Search** dialog box. Select the search criteria by which you want to search and click **OK** to continue or **Clear** to return to the **Recent Calls** page.
- **More Actions** icon—Provides a drop-down list with the following additional actions:

  - **Set Columns**—Enables you to select which columns to display for recent calls. If a call does not contain a piece of information, the Oracle SDM Cloud leaves that cell of the table blank.
  - **Select Device**—Allows you to see recent calls for a specific device.
- **Refresh** icon—Sends an on demand call to the Session Monitor to retrieve call data.

Filter Recent Calls

Click the Recent Call page's **Filters** button to access the Filters dialog box. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows you to create, edit, copy, and delete filters, and to apply filters to the recent calls table.

The Filters dialog contains the following buttons and entry fields:

- **Add** button—Add a new filter. Clicking this button displays the **Add Filter** dialog box. For more information on creating a new filter, see "Create a Filter".
- **Edit** button—Select a filter from the list and click Edit to edit the filter criteria.
- **Delete** button—Deletes the selected filter.
- **Apply** button—Applies the selected filter to the current Recent Calls table. A filter must first be saved before it can be applied.
- **Copy** button—Create a copy of an existing filter that can then be modified. This copy is added to the Filters list.
- **Refresh** icon—Refreshes the list of filters displayed.

The Filters dialog contains 2 columns, Name (the name of the filter) and Creator (the user who created this filter).

Create a Filter

To create a filter that can be applied to the Recent Calls table:

1. Navigate to **Monitoring Manager**, **Calls** and click **Filters**.
   The **Filters** dialog box displays.
2. Click **Add**.
   The **Add Filters** dialog box displays.
3. **Filter name**—Enter a unique name for this filter.
   On the left side of the dialog there is a list of criteria upon which you can filter. When you click on a criteria, the relevant information upon which to filter displays.
4. Select the criteria you want to filter for that instance and either click **Save** to save the filter or **Clear** to discard your changes and return to the previous **Filters** dialog box.

,

Edit a Filter

You can edit an existing filter:

1. Navigate to the **Monitoring Manager**, **Recent Calls** page.
2. Click **Filters**.
   The Filters dialog box displays, listing all of the saved filters.
3. Select the filter to edit and click **Edit**.

4. Update the filter as necessary.
5. Save your changes by clicking **Save**, click **Clear** to clear the filter, or click **Reset** to reset the filter criteria to what it had originally been saved as.

Select a Device From Recent Calls

From the Recent Calls table, you can select the device filter, allowing you to see recent calls for a specific device. This table displays all MEs that the user has access to, even if they are disabled. For disabled MEs, the checkbox and icon are disabled and display the email ID of the user who disabled it. If the user who disabled the device is removed from the system, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) displays Unknown in that field.

View, Export, and Download Call Ladder Diagrams

From the Recent Calls table, you can select a call in the table and render a call ladder diagram, export the ladder diagram, and download the diagram.

Within the ladder diagram you can do the following:

- Hover over each line to see the full message
- Click **View** to select what information displays in the Ladder Diagram

You can also export the call ladder diagram for a call if you are using either Firefox or Chrome as a browser.

From the Firefox browser, you can save a ladder diagram as either HTML or PDF:

- To save as HTML, right-click on the page and select **Save Page As...**.
- To save as a PDF file, right-click and select **Print**, then select **Save as PDF**.

From the Chrome browser, you can currently save a ladder diagram as a PDF only:

- To save as a PDF file, right-click and select **Print** and select **Save as PDF**.

To download a call ladder diagram, select a call in the table and click the **Download Message Flow** icon.

Manage Mediation Engine Recent Call Access

For users with ME Recent Call Access, **User Management** permissions, users can enable or disable their access to ME Recent Calls, as well as configure a length of time that represents a "recent call".

> **Note**
>
> If the user does not have the appropriate user group permissions under **User Management**, the **Admin** selection under the **Monitoring Manager** slider does not display.

To manage ME Recent Call Access permissions:

1. Expand the **Monitoring Manager** slider and select **Admin**.
   The Monitoring Manager Administration page displays.

2. Optionally, select a value for the **Recent Calls Time Range in Seconds**. This defines the Recent Calls time range length in seconds from the current time stamp or from the start timestamp set in filter criteria (if any). The minimum configurable value is 1 second, the maximum value is 2,592,000 seconds, and the default is 900 seconds.
   Users can only view the last 50 recent calls per ME device.

   > **Note**
   >
   > The Current Timestamp value refers to the start timestamp of the latest recent call, however, if multiple ME devices are present, this timestamp refers to the start timestamps of the latest recent call of an ME device.

3. Click the **ME Recent Call Access** button.
   The **ME Recent Call Access Policy** dialog displays, listing all of the ME devices available to return call data. The table contains the following columns:

Disable checkmark	When selected, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) disables that device from returning recent call data. By default, this is unchecked.
Name	The name of the ME to be enabled or disabled.
IP Address	The IP address of the ME.

4. Select the ME devices for which the Oracle SDM Cloud will return call data.
5. Click **Apply**.

3

Device Manager

The **Device Manager** provides a set of tools that allow the user to manage their devices.

The **Device Manager** slider allows you to manage the following Oracle Communications Product Category and Network Function types:

- **Devices**—Add, manage, remove NFs (devices) from Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), and fetch KPIs. Once you add a device, the Device Manager seamlessly provides access to the device.
- **Device Groups**—Device groups provide the ability to create hierarchical logical grouping of devices as per a user's customization.
- **Sites**—Sites represent a device's physical location.
- **Software Upgrade**—Manage device software upgrades.

Manage Network Functions and Devices

Network Functions (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.

Oracle Communications Service Provider Edge and Core Plug-in Product Category and Network Function Types

The following table describes the product category and NF types that are supported in each category.

Table 3-1

Product Category	NF Type	Component Devices
SP Edge & Core	Device	The following standalone component devices are supported: • Oracle Communications Session Border Controller (SBC) • Oracle Communications Session Router (SR) • Oracle Communications Session Load Balancer (SLB) • Oracle Communications Core Session Manager (CSM) • Oracle Communications Subscriber-aware Load Balancing and Route Management (SLRM) • Oracle Communications Mobile Security Gateway (MSG)
Enterprise Edge & Core	Enterprise Session Border Controller (ESBC), Enterprise Communications Broker (ECB)	• Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker
Session Monitor	Mediation Engine	• Oracle Communications Session Monitor (OCSM)

Note

For a comprehensive list of supported NF versions, see "Network Function Model Support" in *What's New*.

Upload a NF Certificate

To upload a Network Function (NF) certificate:

1. Click the **Tools** drop-down list and select **Certificates**.
   A pop-up window displays.
2. Browse to the NF certificate and click **Upload**.
   The certificate is uploaded.

Note

Companies and organizations (public or private) that are not well-known and globally recognized Certificate Authorities (CA) with a global reach are unlikely to be accepted.

Add a Network Function with Devices

Use this task to add a network function (NF) with devices to the default device group or a device group that you created. Once the NF is added successfully, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) is able to communicate with the devices in the NF. Note that when Identity and Access Management (IAM) is started on-premises, it automatically registers with the Oracle SDM Cloud, appearing in the Managed Devices table, and does not need to be manually added with the procedure below.

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 device, and click **Add**.
3. In the **Select Network Function Type** dialog box, select the product plugin Category from the table. Once you have selected a category, the **Network Function Type** drop-down list is populated with appropriate options.

> **Note**
>
> Once you have added a NF to the Oracle SDM Cloud as a specific component type, if you go back and change the original component type from the device's CLI, the Oracle SDM Cloud will not automatically pick up the that change. From the Oracle SDM Cloud, you must remove the device from the Device Manager, ensure the new device is properly installed, and add it back to the Device Manager with the correct component type.

4. In the **Network Function Type** drop-down list, select from the following NF types:
   - **Device**—(Only available for SP Edge & Core) A NF that contains a single standalone device or device high-availability (HA) pair.
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.
Associated Site field	The associated Site for this device.
Primary IP address field	The primary IP address for this device.
Add device to Configuration Manager checkbox	Adds the NF to the Configuration Manager at the same time it is being added to the device manager.
Secondary IP address field	The IP address for the second device, if this device is part of an HA pair.
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 **v2** and **v3**. If you select **v3**, authentication fields for SNMP version 3 appear. See below for more information about these fields. **Note** When a device is configured to communicate using TLS over ACP, the certificate(s) must be imported to the Oracle SDM Cloud using the Tool, Certificate feature. For more information, see "Manage Transport Layer Security Certificates". When you add a device, you must specify whether to manage the device using 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.
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **HMAC192SHA2256** • **HMAC384SHA5126** • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**
SNMPv3 privacy password field	The SNMP version 3 privacy password.
SNMP community name field	The SNMP community is used to indicate to a device that the requests are from a trusted source. Before Oracle SDM Cloud can manage the device, Management Cloud Engine (MCE) IP address needs to be added to an active configured SNMP community on the device. 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.

7. Click **Apply**.

   The NF and its associated device(s) or the NF with the associated device(s) appear in the **Managed Devices** table.

Add a Mediation Engine Network Function with Devices

Use this task to add a Mediation Engine (ME) Network Function (NF) with devices to the default devices group or a device group that you have created. Once the NF is added successfully, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) is able to communicate with the Mediation Engine devices in the NF.

If you are not using the default Home group to add an NF, you must specify a group for the NF. Note that you must import a ME Certificate for Each ME before it can be added in the Device Manager.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices - Group View** pane, select a device group and click **Add**.
3. In the **Select Network Function Type** dialog box, select the product plugin Category from the table. Once you have selected a category, for example, Session Monitor, the **Network Function Type** drop-down list is populated with appropriate options.
4. In the **Network Function Type** drop-down list, select from the following NF types:
   - **Mediation Engine** (for Session Monitor only)
5. Click **Continue**.
6. In the **Add Network Function: Mediation Engine** dialog box, complete the following fields:

Network Function Name field	The NF name that you want to use for the device(s) that you are configuring.
Associated Site field	The associated Site for this device.
IP address field	The IP address for this ME device.
Authorization Token field	The Authorization Token (API key) to authenticate the user to expose REST APIs for this ME device. For information on generating this REST API token, see the OCSM documentation set https://docs.oracle.com/en/industries/communications/session-monitor/index.html.
SNMP agent mode drop-down list	Currently it is v1v2. The SNMP version cannot be changed for an existing device once it is added unless the device is removed and added again later.
Time zone drop-down list	Select the NF's time zone.

7. Click **Apply**.

The NF and its associated device(s) or the NF with the associated device(s) appear in the **Managed Devices** table.

Fetch KPIs For a Device

For devices that are managed under Device Manager and added under Configuration Manager, Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) is able to fetch multi-dimensional Key Performance Indicators (KPIs) for a selected device based on the product type, platform, and software version. When the Oracle SDM Cloud successfully fetches a list of supported KPIs from a device, it displays them in the Dashboard slider menu under **Device Manager**, **Device**, **<selected device>**. Users can then select a KPI and Oracle SDM Cloud populates a table with all of the data associated with that KPI, including the selected device name and the KPI name.

When a user selects a KPI from the slider menu, the Oracle SDM Cloud displays a loading indicator until it receives the data. If it does not receive this KPI data from the device, it retries 5 times, with 1 second in between each try. If, after the 5th try, the Oracle SDM Cloud still does not receive the data, it displays an error message that no KPI data is available on that device. If a device is either not added under Configuration Manager or Oracle SDM Cloud cannot fetch the KPI list for a selected device, Oracle SDM Cloud displays an error message.

> **Note**
>
> Oracle SDM Cloud caches KPI data fetched from the Management Cloud Engine (MCE) for 20 seconds, and continues to fetch the KPI data from the device each time the cache expires.

The Oracle SDM Cloud page displaying KPI data contains the following buttons and fields:

Refresh icon	Refreshes the KPI table contents.
Save to File button	Exports KPI information from Oracle SDM Cloud as a CSV file to the user's local machine. The exported file contains all of the KPI data, regardless if a filter was applied in the UI.
Search field	Allows a user to search for a specific column in the table. If the data in the table is filtered, the search happens across only the filtered data.
Set Columns button	Opens a dialog box displaying all the columns available for that KPI data table. Select or deselect the columns you want to view or hide and click **OK**.
Filter field and drop-down list (only for those KPIs that support filtering)	Optionally, a user can filter the data in the table if that KPI supports filtering. Users can either select from the drop-down list of type in text to display the closest matches.

Supported KPIs

Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports the following KPIs:

- show sessions
- show interface
- show IP connections UDP
- show IP connections TCP
- show sipd agents
- show sipd interface
- show realms
- show sipd methods

> **Note**
>
> The sip-agents and sip-interface objects are not supported on ECB devices.

Show KPIs

To fetch a list of KPIs from a selected device:

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, expand the appropriate group folder hierarchy and select the device for which you want to view KPIs. You can select only one device at a time.
3. Click **Show KPIs**.

> **Note**
>
> If no device is selected, the **Show KPIs** option is disabled.

The Oracle SDM Cloud displays the list of KPIs available for that device.

4. Select a KPI from the returned list.

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.

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.
SNMP agent mode field	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	**Note** This field applies only to SNMP version 1 and 2. The SNMP community is used to indicate to a device that the requests are from a trusted source. Before Oracle SDM Cloud can manage the device, the Management Cloud Engine (MCE) IP address needs to be added to an active configured SNMP community on the device. **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.
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **HMAC192SHA2256** • **HMAC384SHA5126** • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**

SNMPv3 privacy password field	The SNMP version 3 privacy password.
Authorization token field	The Authorization Token (API key) to authenticate the user to expose REST APIs for this ME device.

4. Click **Apply**.

   A success dialog box displays that the NF was changed.

Manage MCE as a Device

Once the Management Cloud Engine (MCE) is added to the Device Manager, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) starts polling regularly to verify connectivity. The green icon shows a device is accessible. When a MCE is shutdown, it is shown in the Managed Devices table as unreachable.

From the Managed Devices table, when you select a MCE and click **Edit**, the Edit Device dialog box is read-only. You can, however, delete a MCE from the table.

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 Device 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 the **More Actions** icon.
3. Select **Move** from the drop-down list.

   The **Move Network Function** dialog box appears.
4. Click the device group folder to which you want to move the NF and click **OK**.
5. In the **Success** dialog box, click **OK**.

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

Search For a Device

1. Expand the **Device Manager** slider and click **Devices**.
2. Click **Search**.
   The Search dialog box displays.
3. Complete any of the following fields:

Name field	The name of the device.
IP Address field	The device's IP address.
Version drop-down list	The software version running on the device.
Platform drop-down list	The platform running on the device.
Product drop-down list	The type of device.
ConnectivityStatus drop-down list	The connectivity status of the device; either **Reachable** or **Unreachable**.

4. Click **OK** to create the search or **Cancel** to exit out and return to the Managed Devices page.
   Once a search is performed, the search criteria displays above the Managed Devices table.
5. Click **Show All** to clear the search criteria and display all devices in the table.

Remove a Network Function

When you remove an NF, all references to the NF in Configuration Manager, Device Manager, Fault Manager, and Security 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 Device 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 **Confirm** 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 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 the **More Actions** icon.
3. From the drop-down list select **Lock** if it is unlocked or **Unlock** if it is locked.
4. 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 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 the **More Actions** icon.
3. Select **Override lock on device** from the drop-down list.
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 the **More Actions** icon.
3. Select **Reboot** from the drop-down list.
4. In the **Confirm** dialog box, click **Yes**.

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

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

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

Manage Transport Layer Security Certificates

TLS can be used by Management Cloud Engine (MCE) for communication to SBC network functions (NF) devices. You can upload entity or trusted certificates required for this communication to Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), and

Oracle SDM Cloud ensures that the MCE trust store is updated with this information. For information on creating a trusted certificate on the SBC, see the SBC's Security Guide for the SBC version you are running: https://docs.oracle.com/en/industries/communications/session-border-controller/index.html.

Trusted certificates use the X.509 cryptographic standard for security validation in public key infrastructure (PKI) that binds public keys with respective identities signed by a certificate authority (CA) or self-signed certificate. The X.509 standard specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

The Transport Layer Security (TLS) feature provides a Single Secure Sockets Layer (SSL) keystore for entity or trusted certificates that are used to authenticate outbound SSL and southbound interface (SBI) TLS communication to applications, product plugins, and their respective NF devices that run on MCE.

MCE communicates with devices using different protocols. For example, ACP, SNMP, SSH, and SFTP to communicate with devices. TLS communication between MCE and devices should be enabled for additional security. Refer to the specifications of your NF devices (client) to determine if a NF devices supports the SBI TLS feature.

Upload a New Certificate

From Oracle SDM Cloud, you can upload a new X.509 certificate from your system to the Oracle SDM Cloud.

1. On the homepage, select **Tools**, **Certificates**.
2. In the **Certificates** dialog box, click **Import**.
3. In the **Certificates** dialog box, complete the following fields:

Name field	The name of the X.509 certificate.
File field	The directory path of the certificate file on your system. Alternately, click **Browse** to navigate to the certificate on your system.

The certificate appears in the **Certificates** dialog box with certificate name, issuer, start date, end date and serial number of the certificate. The changes are propagated to any cluster members.

Delete an Existing Certificate

From Oracle SDM Cloud, you can delete an existing certificate from the Oracle SDM Cloud.

1. On the main menu, select **Tools**, **Certificates**.
2. In the **Certificates** dialog box, select the certificate you want to delete and click **Delete**.
3. In the **Delete** confirmation dialog box, click **Yes**.

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® Session Delivery Management Cloud (Oracle SDM Cloud):

- Green—The Oracle SDM Cloud can reach the device and retrieve information about the device through SNMP.
- Yellow—The Oracle SDM Cloud can reach one of the devices in an HA pair.
- Red—The Oracle SDM Cloud cannot currently reach the device (or cannot contact both devices in an HA device pair).

You can select which columns appear in the **Managed Devices** table by clicking the **More Actions** icon and selecting **Set Columns**. The following columns are available to select:

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.
Redundancy Status	The redundancy status of this device.
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	Serial number of the standalone device or the primary device in an HA deployment.
Description	A brief description of the device.
Group ID	The group element ID.
Object ID	Internal database object ID.

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 icon	Click to refresh the data displayed on the screen for hierarchical groups, NFs and their associated devices.

Expand All/ Collapse All icon	Click to expand or collapse all folders. When you expand folders, the icon becomes the **Collapse All** icon and when you have collapsed the folders, this icon becomes the **Expand All** icon.

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 Session Delivery Management Cloud User 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 **Move**.
3. In the **Move device group** 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 **Confirm** dialog box, click **Yes** to delete the device group.
4. In the success dialog box, click **OK**.

Manage Sites

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) can group Network Functions (NFs) and devices based on their physical location using Sites.

Using the **Device Manager**, **Sites** page, you can add, edit, view details, assign, and delete Sites.

> **Note**
>
> When a Management Cloud Engine (MCE) is registered in UMS, by default the administrator group has full permissions on the MCE. These permissions can be changed by an administrator within the Security Manager.
> Users can view sites associated to the MCE to which they have access. Sites are visible to all users if they are not used by any of the MCEs.

Add Sites

Use this task to create a Site.

1. Expand the **Device Manager** slider, and click **Sites**.
2. In the **Sites** pane, click **Add**.
3. In the Add Site page, enter a **Site name** and, optionally, a brief **Description** of the site.
4. Click **Apply**.

Edit Sites

While the Edit Site page allows you to edit any managed sites on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) it also provides the Registration ID, which is needed when installing and setting up the Management Cloud Engine (MCE), so that the MCE can auto register itself with the Oracle SDM Cloud when it is started.

1. Expand the **Device Manager** slider and click **Sites**.
2. In the **Sites** page, select the Site to edit and click **Edit**.
3. In the Edit Site page, the **Description** field is the only field you can update.
4. Click **Apply**.

View Site Details

You can view details about what each Site contains including their associated Devices, MCEs, and Managed Sites.

Sites can contain one or many Management Cloud Engines (MCEs), NFs, or both. A site that contains at least one MCE is considered a Managed Site. Sites that do not have any MCEs can be assigned to a managed site, which provides management support to all NFs in that site, as long as the MCE on the management site location can communicate to the NF on the other sites.

> **Note**
>
> When you select a site to view the details, the Managed Sites table displays only information for those MCEs for which the user has permissions granted.

1. Expand the **Device Manager** slider and click **Sites**.
2. In the **Sites** page, select the Site to view and click **Details**.
   The **Site details** dialog box displays showing the following information:

Devices:

- Name
- IP Address
- Version
- Platform

OCMCE:

- Name
- IP Address
- Version
- Platform

Managed Sites:

- Name
- Description
- # MCE
- # Device

Assign Sites

1. Expand the **Device Manager** slider and click **Sites**.
2. In the **Sites** page, select the Site to assign and click **Assign**.
   The **Sites are managed by site:** page appears with a list of sites associated with the selected Site.
3. Select the **Selected** checkbox next to the site you want to assign.
4. Click **Apply**.

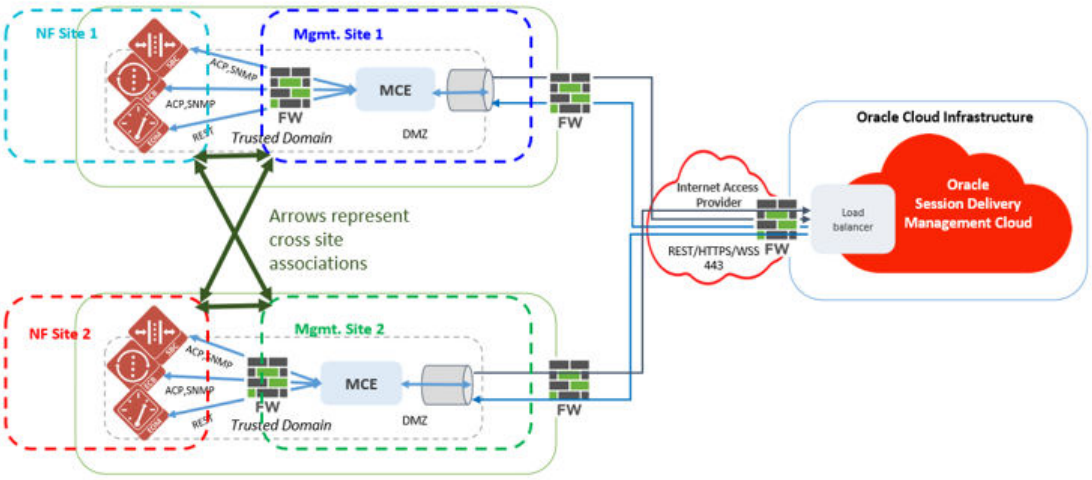
> **Note**
>
> If a Site is linked to an MCE, the site is visible only to users with permissions to view that MCE. However, if a Site is not linked to an MCE, that site is visible to all users.

Delete Sites

1. Expand the **Device Manager** and click **Sites**.
2. In the **Sites** page, select the site you want to delete.
3. Click **Delete**.
4. In the **Confirm** dialog box, click **Yes**.

Multi-Site Model Support

Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports the multi-site model, providing redundancy by allowing managed sites and their Network Functions (NF)s to be associated with multiple MCE Sites.



To enable this deployment model, the following conditions must be met:

- Mgmt Site 1 contains MCEs located at customer location 1.
- Mgmt Site 2 contains MCEs located at customer location 2.
- NF Site 3 contains NFs (for example, SBC, ESBC, ME) located at customer 1 location.
- NF Site 4 contains NFs (for example, SBC, ESBC, ME) located at customer 2 location.
- NF Site 3 and NF site 4 are both assigned to Mgmt Site 1 and Mgmt Site 2.
- MCEs at customer locations can communicate with NFs at both customer locations.
- In the event when either of these MCEs go down, the other MCE can be used to manage the NFs at both Customer Locations 1 and 2.

1. Expand the **Device Manager** slider and click **Sites**.
2. In the **Sites** page, select the Site (containing at least 1 MCE) to which you want to assign NF sites, and click **Assign**.
   The Sites are managed by site: page displays.
3. Select the checkbox for all Sites to assign.
4. Click **Apply**.

For more information on configuring Sites, see **Manage Sites**.

Manage Software Upgrade

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports automated device node (NF) software upgrade across multiple NFs. In order to upgrade, you need to manually upload the software and boot loader images.

> **Note**
>
> All target devices must have the `/code/images/` directory already created prior to the procedure or the work order will fail.

The following sections describe uploading images and managing the software and boot loader image repositories.

Software Image Repository

The Software Image Repository allows you to view and manage all device software images maintained by the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud). The Oracle SDM Cloud supports automated device node (NF) software upgrade across multiple NFs. However, before you can create an upgrade work order, you need to manually upload the software image.

The Software Image Repository displays the Software Image Archive table. The table displays the following information for each image:

Software Image File name	The name of the software image uploaded.
Plugin	The plugin type selected.
Size (Bytes)	The software image file size in bytes.
Date/Time created	The date and time when the file was stored on the Oracle SDM Cloud server.
Version	The software version for the image.
Checksum	The SHA256 checksum for the image. This value is a 64 character string.

To add a software image:

1. Expand the **Device Manager** slider and select **Software Upgrade**, **Software Image Repository**.
   The Software Image Archive screen displays, showing all of the Software Images currently stored in the repository. This page contains the following buttons and icons:
   - **Add** button - Allows you to load a new software image from your local machine to the Oracle SDM Cloud server.
   - **Delete** button - Deletes a selected software image. The Oracle SDM Cloud only allows you to delete software images that are NOT associated with a work order and displays an error if a user attempts to delete such a software image.
   - **Refresh** icon - Refreshes the Software Image Archive table.
2. Click **Add**.
   The **Upload Software Image to Archive** dialog appears.
3. Select the Network Function **Category** from the Categories table (either **SP Edge & Core** or **Enterprise Edge & Core**). Click **Browse** and browse to your locally saved copy of the software image.
4. Click **Upload**.
   The file you uploaded appears in the Software Image Archive table.

Delete a Software Image

To remove a software image you no longer need to store in the Software Image Repository:

1. Expand the **Device Manager** slider and select **Software Upgrade**, **Software Image Repository**.
2. Select the software image you want.
3. Click **Delete**.

4. In the Confirm dialog box, click **Yes**. The software image is removed from the Software Image Archive table.

> **Note**
>
> When deleting a software image, Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) does not allow you to delete an image if it is being used by any reachable devices, whether or not the user has access to it.

Boot Loader Image Repository

The Boot Loader Image Repository allows you to view, load, and delete all device boot loader images maintained by the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud). The Oracle SDM Cloud supports automated device node (NF) boot loader upgrade across multiple NFs. However, before you can create an upgrade work order, you need to manually upload the boot loader image.

The Boot Loader Image Repository displays the Boot loader Image Archive table. The table displays the following information for each image:

Boot Loader Image File name	The name of the boot loader image uploaded.
Plugin	The plugin type selected.
Size (Bytes)	The boot loader image file size in bytes.
Date/Time created	The date and time when the file was stored on the Oracle SDM Cloud server.
Version	The boot loader version.
Checksum	The SHA256 checksum for the image. This value is a 64 character string.

To add a boot loader image:

1. Expand the **Device Manager** slider and select **Software Upgrade**, **Boot Loader Image Repository**.
   The Boot Loader Image Archive screen displays, showing all of the Boot Loader Images currently stored in the repository. This page contains the following buttons:
   - **Add** button- Allows you to add a new boot loader image from your local machine to the Oracle SDM Cloud server.
   - **Delete** button - Deletes a selected boot loader image. The Oracle SDM Cloud only allows you to delete boot loader images that are NOT associated with a work order and displays an error if a user attempts to delete such a boot loader image.
   - **Refresh** icon- Refreshes the Boot Loader Image Archive table.
2. Click **Add**.
   The **Upload Boot Loader Image to the Archive** dialog appears.
3. Select the Network Function **Category** from the Categories table (either **SP Edge & Core** or **Enterprise Edge & Core**). Click **Browse** and browse to your locally saved copy of the boot loader image.
4. Click **Upload**.
   The file you uploaded appears in the Boot Loader Image Archive table.

Delete a Boot Loader Image

To remove a boot loader image, you no longer need to store in the Boot Loader Image Repository:

1. Expand the **Device Manager** slider and select **Software Upgrade**, **Boot Loader Image Repository**.
2. Select the boot loader image you want.
3. Click **Delete**.
4. In the Confirm dialog box, click **Yes**. The boot loader image is removed from the Boot loader Image Archive table.

> **Note**
>
> When deleting a boot loader image, Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) does not allow you to delete an image if it is being used by any reachable devices, whether or not the user has access to it.

4

Security Manager

With administrator privileges, Security Manager allows you to do the following:

- Create and manage user groups.
- Configure security authorization levels, policies and privileges for user groups.
- Provide specific access controls for individual user groups, views, and operations.
- Limit access to specific features and functionality for specific users.
- Configure audit log parameters.

Configure User Groups

A user group is a logical construct that the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) uses to specify the authorization privileges that users assigned to certain groups inherit. Oracle SDM Cloud automatically adds the roles directly to the user roles on the Identity and Access Management (IAM) portal.

The Oracle SDM Cloud provides three default User Groups.

- Administrators
- Provisioners
- Monitors
  While you cannot modify the default User Groups, you can add and modify customized User Groups to create your own authorization policies. When you add a new User Group, Oracle SDM Cloud automatically adds the group to your IAM.

> **Note**
>
> Do not add a new role to your Oracle SDM Cloud application through IAM. If you require a new role on the Oracle SDM Cloud application, add a new group using Security Manager in Oracle SDM Cloud.

Add a User Group

Once you've added a new user group in the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), which will appear as a new role in Identity and Access Management (IAM) and Access Management (IAM). Once you have assigned a user to a role, that user will inherit the group-based privileges.

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. On the **User Groups** page, click **Add**.
3. On the **Add Group** screen, complete the following fields:

Group name field	The user group name. Use the following guidelines for naming this group:

	• Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique. • This name cannot contain spaces.
Group permissions copy from drop-down list	Copy existing privileges by choosing from the following default user groups. By selecting a user group from this drop-down, the privileges from the selected group are copied to the newly created group. By default, if no value is selected, the group is created with all privileges set to **None**. • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **provisioners**—This group is privileged to configure Oracle SDM Cloud and save and apply the configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle SDM Cloud, and has the fewest privileges. **Note** This value creates a copy of privileges to be applied to the new group. However, once a group is created, you can go back and customize those privileges at any time.

4. Click **Apply**.

   You are returned to the User Groups table where the new user group has been added. If you navigate to your IAM portal, you will see a new user role for that security group has already been added.

Delete a User Group

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. On the **Groups** page, choose the (non-default) user group that you want to delete from the **User Groups** table and click **Delete**.
3. In the **Delete** confirmation dialog box, click **Yes** to delete this user group.

   The user group is removed from the **User Groups** table.
4. In the success dialog box, click **OK**.

Apply or Change User Group Privileges

You can apply privileges to user groups that you add to allow or deny all users within this user group the ability to perform certain operations. This includes items intended for use with separate Oracle SDM Cloud managers. For the default **administrators**, **provisioners**, and **monitor** user groups, only device group privileges can be changed.

User group privileges that are assigned to the **administrators** user groups inherit most of the same access privileges.

All user group privileges that are available through Oracle SDM Cloud are described in the following sections.

Apply User Group Privileges for Configuration

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. In the expanded group pane, click the **Configuration** tab and click the folder and subfolder sliders to expand the item operations list.
4. Select the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, select the following user group privilege options for folders or items in the **Configuration** tab table described below:
   - **Full**—Allowed to perform administrative operations.
   - **None**—Not allowed to perform administrative operations.
   - **View**—Allowed to monitor only.

> **Note**
>
> The fields described below appear if all features are enabled.

Configuration folder	Set privilege levels for all configuration operations.
Device configuration folder	Set privilege levels for all of the following user management operations accessible on the **Configuration Manager** slider.
Configure services item	Set privilege levels for host-in-path (HIP) firewall functions that are allowed to pass administrative traffic to the host.
Configure interfaces item	Set privilege levels for FTP, ICMP, SNMP, Telnet, and SSH interfaces.
Configure NM controls item	Set privilege levels for network management controls performance group pane.
Configure security item	Set privilege levels for the Security Manager features.

Configure system item	Set privilege levels for the configuration of system usage parameters.
Offline Configuration item	Set privilege levels for offline configuration functionality.
Load device item	Set privilege levels for loading a device.
Override lock item	Set privilege levels for overriding a lock on a device.
Transfer configuration view item	Set privilege to transfer user device configuration modifications from one user to another.
Update to device item	Set privilege levels for saving and activating the configuration of a device.
Configuration archive item	Set privilege levels for backing up configurations, restoring configurations, and deleting archived configurations in the configuration archive.

6. Click **Apply**.

Apply User Group Privileges for Device Maintenance

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Select the **Device Maintenance** tab to modify user group privileges and click on the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Device Maintenance** tab table described below:
   - **Full**—The user group is allowed to reboot a device.
   - **None**—The user group is not allowed to reboot a device.
   - **View**—The user is allowed to view reboot device work orders.

Reboot	Reboot the device.
Override Lock On Device	Override the lock on a device.
Software Upgrade	Create, delete, or modify software upgrade work orders.

6. Click **Apply**.

Apply User Group Privileges for the Administrative Operations

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. In the expanded group pane, click the **Administrative operations** tab and click the folder and subfolder sliders to expand the item operations list.

4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Administrative operations** tab table described below:
   - **Full**—(Default) Allowed to perform administrative operations.
   - **None**—Not allowed to perform administrative operations.

Administrative operations folder	Set privilege levels for all of the following administrative operations.
Security administration folder	Set privilege levels for all of the following user management operations accessible on the **Security Manager** slider.
Group operations item	Set privilege levels to add a new user group, modify and delete existing user groups from Security Manager.
Device group item	Assign privileges for all functions pertaining to a device group within the Device Manager, including adding, deleting, moving, and renaming a device group.
Device item	Assign privileges for the following device operations: • Add a new device • Move and delete an existing device accessible through the Device Manager and Configuration Manager sliders
View all audit logs item	View all audit logs.
View own audit log item	View only personal audit log.
Change audit log auto purge interval item	Configure the number of days of audit logs to keep.
Export audit logs item	Export all of an audit log to a file.
Manual audit log purge item	Manually purge audit logs.
Site item	Create and manage Sites.

6. Click **Apply**.

Apply User Group Privileges for Fault Management Operations

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Fault management** tab and click the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Fault management** tab table described below:

- **Full**—Allowed to perform event or alarm operations.
- **None**—Not allowed to perform event or alarm operations.
- **View**—Allowed to monitor only.

Fault management folder	If the **None** privilege is chosen, the **Fault Manager** slider does not appear in the Oracle SDM Cloud GUI.
Events and Alarms folder	Assign the privileges for all of the following event and alarm operations accessible on the **Fault Manager** slider.
Alarms item	Assign the privileges for the alarm operations - delete alarms and edit the alarm severity levels accessible under the **Alarms** and **Trap Event Settings** tabs.
Events item	Assign the privileges for the event operations - delete events accessible under the **Events** tab.

6. Click **Apply**.

Apply User Group Privileges for Device Groups

Use this task to apply user-group privileges for device groups that appear on the **Device Manager** slider.

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Device groups** tab.
4. In the **Device groups** box table, complete the following fields:

Include children check box	(Optional) Check the check box to select all children of the device group. Next select either **Set all to None** or **Set all to Full** have no privileges or full privileges respectively for the children of the device group.
Set all to None button	Set all Device groups to have no privileges.
Set all to Full button	Set all Device groups to have full privileges.

   The **Preview** box displays the device group based on the privileges that are assigned (**Full**, **View**, **None**).
5. Repeat the previous step for other device groups (if there are any).
6. Click **Apply**.

Apply User Group Privileges for Application Management Operations

Use this task to apply user-group privileges for application management operations.

1. Expand the **Security Manager** slider and select **User management**, **Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Applications** tab and select the folder and subfolder sliders to expand the item operations list.

4. In the operations table, locate the item you want to configure. In the **Privileges** column, select a privilege level from the drop-down list.
   - **Full**—Allows all application management operations
   - **View**—Allows monitoring only
   - **None**—Disables access to application management operations
5. Configure privileges for the following folders and items as needed:

Applications folder	Allows access to **Dashboard Manager**, **Monitoring Manager**, and **Route Manager** options in the slider menu.
Dashboard Manager folder	Assign privileges for all dashboard and portlet customization operations available under the **Dashboard Manager** slider.
Dashboard Customization item	Allows access to the dashboard designer and portlet designer to customize dashboards and portlets.
Monitoring Manager folder	Assign privileges for all of the following operations related to monitoring an Oracle Communications Session Monitor (OCSM).
Calls item	Assign privileges for filter operations—such as add, edit, delete, copy, and apply—used in the **Recent Calls** table under the **Monitoring Manager** option.
Admin folder	Assign privileges for the following administrative operations. If **None** is selected, the **Admin** option is not displayed under **Monitoring Manager**.
ME Recent Call Access item	Allows the user to disable the Mediation Engine (ME) and to set the time range to fetch the recent calls from OCSM.
Route Manager folder	Assign the privileges for the following managing routes operations.
Route set item	Allows access to manage routes, route sets, templates, and device associations.

6. Click **Apply**.

Audit Logs

You can use the audit log (containing audit trails) generated by Oracle SDM Cloud to view performed operations information, which includes the time these operations were performed, whether they were successful, and who performed them when they were logged into the system.

> **Note**
>
> Audit logs contain different information depending on the feature functionality.

Audit trails include the following information:

- The user who performed the operation.
- What operation was performed by the user.
- When the operation was performed by the user.
- Whether the operation performed by the user was successful or failed.

View and Save an Audit Log

The audit log tracks user-initiated events. The following list describes some examples of user events that are audit logged in Oracle SDM Cloud:

- User logins and logouts.
- Managed devices are added.
- Device groups are added.
- Oracle Communications Session Delivery products are loaded.
- An element is added, deleted, or modified.
- A device is rebooted.
- Configurations are saved or activated.

1. Expand the **Security Manager** slider and select **Audit log**, **View**.
2. In the **Audit log** pane, click **Set Columns** to select all columns you want to view in the Audit Log table. The following table lists and describes all columns available view:

Username field	The name of the user who performed the operation.
Time field	The time stamp for when the operation was performed by the user.
Category field	The category of operation performed by the user. For example, Authentication.
Operation field	The specific operation performed by the user.
Status field	The status of the operation performed by the user, whether it was successful or failed.
Device field	The name of the device that the user performed an operation upon.
Network function field	The NF name.
Description field	The description of the operation performed.
Sequence number field	The audit log reference number.

3. Click **OK** to accept your selections or **Reset** to close the **Set Columns** dialog box and ignore any changes.

4. To see details for a specific user entry, select an entry row in the table and click **Details** or double-click the row.

   In the **Audit log details** dialog box, the information described in the table above is displayed for the specified user entry.

5. Click **OK**.
6. Click **Save to file** to open the audit log file or save it to a file.

> **Note**
>
> The downloaded CSV file is limited to 250 entries.

Search the Audit Log

1. Expand the **Security Manager** slider and select **Audit log**, **View**.
2. In the **Audit log** pane, click **Search**.
3. In the **Audit Log Search** dialog box, complete some or all of the following fields to search the audit log:

Username field	Choose the name of the user who performed the operation.
Category drop-down list	Choose the category of operation performed by the user. For example, Authentication.
Operation box	Chose the specific operation performed by the user.
Device	The name of the device that the user performed an operation upon.
Status	The status of the operation performed by the user, whether it was successful or failed.
Start Time	Choose a start time from the calendar.
End Time	Choose an end time from the calendar.

4. Click **OK**.

Schedule Audit Log Files to be Purged Automatically

1. Expand the **Security Manager** slider and select **Audit log**, **Purge**.
2. In the **Purge audit logs** pane, specify the number of days of audit logs that are kept in the **Interval in days** field. The minimum configurable value is 2 days.
3. Click **Apply**.

IAM

The Identity Access Management page provides unique IDs needed to connect the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) to the Identity and Access Management (IAM). The IDs provided include the following:

- Oracle SDM Cloud FQDN

- Oracle SDM Cloud Tenant ID
- IDCS FQDN
- IDCS Tenant ID
- Management Cloud Engine (MCE) IDCS client ID
- MCE IDCS client secret
  This information is required as input when installing and setting up the MCE on-premises. For more information, see the Oracle SDM Cloud *Installation Guide*.

5
Configuration Manager

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

Associate Devices with Oracle SDM Cloud

While the NFs added to the Device Manager are entered into the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) inventory, these devices are not automatically managed. You must add the NF to Configuration Manager, informing Oracle SDM Cloud that the NF has been targeted for management. Upon being added to Configuration Manager, Oracle SDM Cloud allows configuration provisioning to the device, starts periodically polling the device for health metrics, and accepts traps or alarms from devices to manage and store in Fault Manager.

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 you want to associate with Oracle SDM Cloud, and click **OK**. You are returned to the Managed Devices page.

   The entire NF folder hierarchy, including the NF appears in the **Selected devices** table and the device is now associated with the Oracle SDM Cloud. Use the **>** button to move the associated node.

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

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.

Users are able to see only the devices to which they have access per their Security Manager User Group Permission. For more information see "Apply or Change User Group Privileges" in the Security Manager chapter.

> **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. On the **Managed Devices** page click the **More Actions** icon and select **Set Columns**. The following table describes all of the columns available to view:

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.
Redundancy Status	Whether the device is standalone or part of an HA pair.
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 fetched from 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	The device IP address of the device. The IP address is displayed depending on the details added by the user in the **Device Manager**.
Target Name	The device target name.
Category	The element manager (EM) plug-in product vendor category.
Product	The device product.
Product Key	The device product key.
Plugin Name	The name of the plugin being used.
Vendor	The plugin vendor to which the devices belong.
Device Config Id	The identity provided by the plugin. For example, the device identity for the plugin is its target name.
Object ID	The internal database object ID.
Group ID	The parent group ID.

Search For a Device in Configuration Manager

1. Expand the **Configuration Manager** slider and click **Devices**.
2. Click **Search**.
   The Search dialog box displays.
3. Complete any of the following fields:

Name field	The name of the configuration.
IP Address field	The device's IP address.
Version drop-down list	The software version running on the device configuration.
Platform drop-down list	The platform running on the device configuration.
Product drop-down list	The type of device associated with this configuration.

4. Click **OK** to create the search or Cancel to exit out and return to the Managed Devices page.
   Once a search is performed, the search criteria displays above the Managed Devices table.
5. Click **Show All** to clear the search criteria and display all devices in the table.

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® Session Delivery Management Cloud (Oracle SDM Cloud) 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 SDM Cloud 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.

The Oracle SDM Cloud's Configuration Management is model-driven based on the configuration models supported for each Network Function (NF). Therefore, the configuration navigation tree and the configuration screens are rendered dynamically based on the NF supported configurations for each product, version, and platform that Oracle SDM Cloudcan manage. The Configuration navigation tree lists the relevant configuration element names in alphabetical order. On selecting a configuration element from the navigation tree, the attributes for this element are rendered dynamically with additional information on each attribute to allow modifications to be made. For more information on specific configuration elements and attributes, refer to the appropriate configuration user guide for that product.

- For SBC related products, see SBC documentation: https://docs.oracle.com/en/industries/communications/session-border-controller/index.html
- For E-SBC related products, see E-SBC documentation: https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/index.html
- For Oracle Communications Session Monitor (OCSM), currently Configuration Manager does not support Mediation Engine configuration. For information on configuring the OCSM, see https://docs.oracle.com/en/industries/communications/session-monitor/index.html
- For ECB related products, see ECB documentation: https://docs.oracle.com/en/industries/communications/enterprise-communications-broker/index.html

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**.

   The NF configuration is loaded.

> **Note**
>
> The time it takes to load a configuration depends on the number of configuration elements on the device. Larger configurations may take longer.

Configure a Configuration Element

Use this task to configure a configuration element.

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

   This renders the table with the list of devices managed by the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) (for example, the Managed Devices Table) which have previously been added to Configuration Manager. For information on adding a loading a configuration, see "Load the Configuration of a Local Device to Configure a Device".

2. In the **Managed Devices** Table, select a device and click **Load**.

   The load process ensures that a local copy of the device configuration is loaded into the Oracle SDM Cloud database, allowing configuration modification and validation on the most current device configuration. If successful, the navigation tree lists the configuration elements that can be configured for the selected device product, version, and platform.

   The selected device is loaded and shown.

3. In the navigation panel, click the configuration element to edit.

   This renders the possible configuration attributes for the configuration element in the main body. If the attribute is a multi-instance value, the Oracle SDM Cloud displays a table and if it is a scalar value, a label and text box. Tool tips and additional attribute information hints are also provided.

4. Target an attribute and create, update, or delete content as needed.

5. Click **Apply** to complete your changes.

   This stores the updates to your own personal configuration workspace on Oracle SDM Cloud. Other users cannot see your changes until you perform an update to the device. For information on updating a device, see "Update a Device Configuration".

> **Note**
>
> If using the ECB dialing-context feature, the dialing-context screen displays the nested tree structure data, and you cannot add the first dialing-context, or its immediate parent, under the type geographic and corporate, as it is not supported.

Update a Device Configuration

Pre-requisites: Before you update a device configuration you must first load it in Configuration Manager.

> **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 the 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

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. Select the **User** for which you want to view Devices.
3. 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.
4. 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.

5. 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 Change button	Select a change row and click to undo selected changes.
Change Owner	Click to transfer the ownership of your changes to another user. **Note** This button is disabled under the following circumstances: • When the **User** drop-down value is set to `All` • When the Group to which the User belongs has the permission for **Transfer Configuration View** set to `None`.
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.

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, click the **More Actions** icon, 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**.

View Device Tasks

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, click the **More Actions** icon, and select **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.

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, click the **More Actions** icon, and click **View Changes**.
3. In the **Configuration changes** pane, click **Save to File**.

Remove Device Association with Oracle SDM Cloud

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 **Selected Devices** pane, expand the folder hierarchy and click the network function (NF) device you want to remove.
4. Click the remove arrow button to move the selected device to the **Available Devices** pane.
5. Click **OK**. Your device is no longer associated with Configuration Management and appears in the **Device list** pane.

   By removing a device association from the Configuration Manager, this device is no longer polled for statistics and all traps generated from this device remain unprocessed.

Manage Golden and Offline Configurations

The Golden/Offline Configurations page allows you to view, add, edit, load (offline configurations only), copy, and delete both golden and offline configurations in the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

In addition to offline configurations, Oracle SDM Cloud supports the use of 'golden configurations'. A golden configuration is a baseline configuration known to work well. It is used to compare other configurations and report any errors or discrepancies.

> **Note**
>
> If there is a device reference in the Golden/Offline configurations, the access to that configuration is dependent upon whether the user has access privileges to the referenced device or not.
> However, if there is no device reference within the configuration, then the user is able to view and modify all Golden/Offline configurations created and updated by any user from the same group.

When you select a golden configuration from the table, the following buttons and actions are disabled:

- View Data Variable
- View Changes
- Copy
- Generate template
- Generate Spreadsheet
- Update Device
- Override Lock

1. Expand the **Configuration Manager** slider and select **Configuration Tools**, **Golden/ Offline Configurations**.
2. Click **Set Columns** to select the columns to view in the Golden/Offline Configuration table. The following table describes the columns available to view:

Name	Name of the configuration.
Software Version	Software version of the configuration.
Platform	Platform of the configuration.
Description	Description text for the configuration.
Created Date	The UTC date and time at which the configuration was created.
Last Modified Date	The UTC date and time at which the configuration was last modified.
Category	Category type of the configuration.
Component	Component type of the configuration.
Plugin Name	Plugin name of the configuration.
Vendor Name	The Vendor Name of the configuration.
Product Name	The Product Name of the configuration.
Redundancy Type	The Redundancy Type of the configuration.
Configuration Type	The type of configuration created; either Golden or Offline.

Device Reference	The device associated with the configuration.

The Golden/Offline Configuration page contains the following buttons and icons:

Add button	Adds a new offline configuration. Clicking this button launches the **Add offline configuration** page.
Load button	Loads configuration elements and attributes for the selected configuration. This updates the navigation tree, adding the child group to the configuration group and populating all element groups.
Search button	Launches the **Search** dialog box, allowing users to search for either a golden or offline configuration based on specified criteria.
Show All button	Clears the search and displays all golden and offline configurations.
More Actions icon	Provides a drop-down list with the following additional actions for a selected offline configuration: • **View Changes** - Launches the Local configuration view page for the selected offline configuration, displaying the modifications made to that configuration. • **View Data Variable** - Launches the Data Variables page for the selected offline configuration. For more information on data variables, see "Create Data Variables to Support Device Specific Values". • **Copy** - Launches the Copy Offline Configuration dialog box, to create a copy of the selected offline configuration. • **Generate Template** - Downloads or exports a spreadsheet template, of the selected offline configuration, in CSV format. • **Generate Spreadsheet** - Launches the Generate Spreadsheet For Offline Configuration page for the selected offline configuration. You must generate a spreadsheet for any newly created Data Variables. • **Delete** - Deletes the selected offline configuration.

	• **Update Device** - Launches the Add Device Configuration Work Order Wizard for the selected offline configuration. • **Override Lock** - Overrides a lock set on an offline configuration by another user. • **Edit** - Edit the configuration of the selected row. • **Set Columns** - Select the columns displayed in this table.
Refresh icon	Refreshes the table's contents.

Add an Offline Configuration

You can add an offline configuration by using either a device configuration file, a managed device, an archived configuration, or a software version. Before adding an offline configuration, ensure you have a copy of a Data Doc saved to your server.

You can add an offline configuration by importing a Data Doc. A Data Doc can be one of the following:

- Device configuration file
- Based on a software version
- The configuration of a managed device
- A configuration archive

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:

Golden configuration checkbox	Ensure this field is left unchecked when adding an offline configuration (not a golden configuration).
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.

Configuration seeded from drop-down list	Select one of the following: • **Device configuration file** • **Managed device** • **Archived configuration** • **Software version**
Selected configuration file Browse button	When the **Configuration seeded from** value is set to **Device configuration file**, browse to the Data Doc device configuration file saved to your server.
Selected managed device Browse button	When the **Configuration seeded from** value is set to **Managed device**, this launches the **Select managed device** dialog. Select the device you want and click **Apply**.
Selected Archive Configuration Browse button	When the **Configuration seeded from** value is set to **Archived configuration**, this launches the **Select Archive Configuration** dialog. Select the archived configuration you want and click **Apply**.
Category field	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 drop-down list	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.
Software Version drop-down list	When the **Configuration seeded from** value is set to **Software version**, selected the supported software version from the drop-down list.
Entitlements browse button	Launches the **Entitlements** dialog box, allowing you to set the entitlements for this offline configuration.

4. Click **Apply**.
   The Oracle SDM Cloud loads and saves the selected configuration file.

Add a Golden Configuration

You can add a golden configuration by importing a Data Doc. A golden configuration can be seeded from one of the following types:

- Device configuration file
- Managed device
- Archived configuration
- Offline configuration

Users can create multiple golden configurations from the same source.

1. On the **Configuration Manager** slider, select **Configuration Tools**, **Golden/Offline Configurations**.
2. In the **Golden/Offline Configuration** tab, click **Add**.

3. In the **Add Golden/Offline Configuration** page, complete the following fields:

Golden configuration checkbox	Click this checkbox when adding a golden configuration (not an offline configuration).
Configuration name field	The unique golden 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	A brief description of the golden configuration.
Configuration seeded from drop-down list	Select one of the following: • **Device configuration file** • **Managed device** • **Archived configuration** • **Offline configuration**
Selected configuration file Browse button	When the **Configuration seeded from** value is set to **Device configuration file**, browse to the Data Doc device configuration file saved to your server.
Selected managed device Browse button	When the **Configuration seeded from** value is set to **Managed device**, this launches the **Select managed device** dialog. Select the device you want and click **Apply**. Once a device is selected, the values for **Category**, **Component**, **Platform**, and **Software** version are automatically populated and disabled.
Selected Archive Configuration Browse button	When the **Configuration seeded from** value is set to **Archived configuration**, this launches the **Select Archive Configuration** dialog, which contains a table of existing archived configurations. This table contains the **Filter** field to filter the archived configurations by device. Select the archived configuration you want and click **Apply**. Once an archived configuration is selected, the values for **Category**, **Component**, **Platform**, and **Software** version are automatically populated and disabled.
Selected Offline Configuration Browse button	When the **Configuration seeded from** value is set to **Offline configuration**, this launches the **Select Offline Configuration** dialog, which contains a table of existing offline configurations. Select the offline configuration you want and, if there are spreadsheets associated, select a spreadsheet. Select a device that is added to the Configuration Manager click **Apply**. Once an offline configuration is selected, the values for **Category**,

	Component, **Platform**, and **Software** version are automatically populated and disabled.
Category field	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 drop-down list	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.
Software Version drop-down list	Select the supported software version from the drop-down list.

4. Click **Apply**. The Oracle SDM Cloud loads and saves the golden configuration file.

Reseed a Golden Configuration

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports reseeding golden configurations, meaning you can update the source from which a golden configuration is derived.

> **Note**
>
> If you select a golden configuration that has a device reference, **Device configuration file** is not an option in the **Reseed type** drop-down list.

1. Expand the **Configuration Manager** slider and click **Configuration tools**, **Golden/Offline Configurations**.
2. In the **Golden/Offline Config** tab, select the golden configuration you want to reseed from the table, click the **More Actions** icon, and select **Edit**.
3. In the **Edit Golden/Offline Configuration** screen, click the **Reseed golden configuration** checkbox.
   Enter values for the following parameters:

Reseed type drop-down list	Select the type of Data Doc to reseed the golden configuration. • Managed device • Device configuration file • Archived configuration • Offline Configuration
Selected managed device browse button	When the **Reseed type** value is set to **Managed device**, this launches the **Select managed device** dialog. This dialog displays a list of valid managed devices that have the same category and device reference as that of the selected golden configuration. Select the device you want and click **Apply**. Once a device is selected,

	the values for **Category**, **Component**, **Platform**, and **Software version** are automatically populated and disabled.
Selected device configuration file browse button	The **Device configuration file** option is only available if the golden configuration does not contain a device reference. When the **Reseed type** value is set to **Device configuration file**, browse to the Data Doc device configuration file saved to your server. Once a device is selected, the value for **Category** is automatically populated and disabled.
Selected Archive Configuration browse button	When the **Reseed type** value is set to **Archived configuration**, this launches the **Select Archive Configuration** dialog. If the selected golden configuration is associated with a device reference, the dialog displays a list of valid archived configurations matching the category and device reference. If the selected golden configuration is not associated with a device reference, the dialog displays a list of valid archived configurations matching the product type of the golden configuration. This table contains the **Filter** field to filter the archived configurations by device. Select the archived configuration you want and click **Apply**. Once an archived configuration is selected, the values for **Category**, **Component**, **Platform**, and **Software version** are automatically populated and disabled.
Selected Offline Configuration browse button	When the **Configuration seeded from** value is set to **Offline configuration**, this launches the **Select Offline Configuration** dialog, which contains a table of valid offline configurations that meet the following criteria: • If the offline configuration was created by the managed device or archived configuration, then the device reference and component are checked to match with the selected golden configuration. • If the offline configuration was created by the device configuration file or software version, the component value is checked to match with the selected golden configuration. Select the offline configuration you want and, if there are spreadsheets associated, select a spreadsheet. Select a device that is added to the Configuration Manager and

	click **Apply**. Once an offline configuration is selected, the values for **Category**, **Component**, **Platform**, and **Software version** are automatically populated and disabled.
Category browse button	Select the plug-in product vendor category.
Component drop-down list	The default NF component delivered by the plug-in product vendor category.
Platform drop-down list	Select the device hardware version to reseed the configuration from a device template.
Software Version drop-down list	Select the supported software version from the drop-down list.

4. Click **Apply**. The Oracle SDM Cloud prompts you to confirm the action.
   The Oracle SDM Cloud displays a success message if reseeding is successful, or an error message if any errors are encountered.

Generate a Spreadsheet Template

To use the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) spreadsheet for multiple device configuration files, you must generate a spreadsheet template.

To generate a spreadsheet template:

1. On the **Configuration Manager** slider, select **Configuration Tools**, **Offline Configuration**.
   The Offline Configuration Spreadsheets page displays.
2. Click the **More Actions** icon and select **Generate Template** from the drop-down list.
   The Oracle SDM Cloud downloads a file in csv format to save the spreadsheet template. This template contains the header fields corresponding to device details and the bind variables based on the selected Offline Configuration.

> **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 Oracle SDM Cloud performs validation checks on all associated spreadsheets and marks any spreadsheets invalid that fail. When you generate a template, the Oracle SDM Cloud 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 contains the following fields separated by a comma.

Table 5-1 Offline Config Headers

Header	Description	Mandatory
Device Name	The name of the device to be exported.	Yes
Primary IP Address	The primary IP address of the device. The value must be a valid IP address.	Yes
Secondary IP Address.	The secondary IP address of the device. The value must be a valid IP address.	No
Bind variable...1 Name	This field corresponds to the bind variable in the Offline Configuration. The type will be the same as bind variable type.	No. This is dependent on the Offline Configuration.
Bind variable...2 Name	This field corresponds to the bind variable in the Offline Configuration. The type will be the same as bind variable type.	No. This is dependent on the Offline Configuration.
Bind variable...3 Name	This field corresponds to the bind variable in the Offline Configuration. The type will be the same as bind variable type.	No. This is dependent on the Offline Configuration.

Upload a Spreadsheet

Once you have generated a template and entered the required device information, you must upload it to Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

1. On the **Configuration Manager** slider, select **Configuration Tools**, **Offline Configurations**.
2. Click the **Spreadsheets** tab.
3. Click **Upload**.
   The **Upload OC bind variable spreadsheet** dialog box appears.
4. In the dialog box enter a **Name** for the spreadsheet, browse to the location of the file, and click **Upload**.
   Upon clicking Upload, the Oracle SDM Cloud checks the following conditions to ensure the file is valid:
   - The file is in csv format with a .csv as a file extension.
   - The first row of the file is formatted properly. See "Generate a Spreadsheet Template" for more information.

- The file is associated with and properly matches an existing Oracle SDM Cloud 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.
- No new columns may be added to the spreadsheet.
- The order of rows and columns in the template must match against the offline configuration that generated the template.
- The user myst have access to the device's name, primary IP Address, secondary IP Address, nand Offline Configuration.
  If any of the validations fail, the upload fails, displaying an error and the details are added ot the log file.

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

Manage Device Deployment Spreadsheets

You can access the spreadsheets generated by the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) to upload, edit, download, and delete.

Access to spreadsheets are as follows:

- Users have read-only access to spreadsheets associated with devices to which they do not have access.
- Users are only able to access spreadsheets with Offline Configurations to which they have access.
- Users can only add devices to which they have access to spreadsheets to which they have access.
- Within spreadsheets, users are only allowed to modify device details to which they have access.

To manage device deployment spreadsheets, navigate to **Configuration Manager**, **Configuration Tools**, **Offline Configurations**. Select the **Spreadsheets** tab.

The Oracle SDM Cloud applies the following rules when creating and or updating Data Variable (DV) values within spreadsheets:

- If you generate a spreadsheet with all DVs set to the default value, you do not have to go to every device to configure it as they are updated automatically.
- If you add a DV set to the default value, the existing spreadsheets are updated automatically and remain in the 'configured' state.
- While either generating a spreadsheet with DVs or updating DVs, if the DVs are not all set to the default values, no automatic updates occur. You must edit and configure the spreadsheet for every device manually.

Click the **Set Columns** button to select the columns you want displayed in this table. The following table describes all columns available to view:

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.
Status	The status of the spreadsheet. The **Update** button is enabled based on the status of the selected spreadsheet.
Uploaded File	The uploaded file that this spreadsheet is associated with.

The following buttons allow you to manage the Oracle SDM Cloud's spreadsheets:

Button	Description
Upload button	Upload a new spreadsheet.
Download button	Download the highlighted spreadsheet.
Search button	Allows you to search for an offline configuration spreadsheet based on any of the following criteria: • Name • Offline Config • Software Version • Platform
Show All button	Clears search criteria to display all spreadsheets in the table.
More Actions icon	Provides a drop-down list with the following additional actions: • **Delete**:Delete the highlighted spreadsheet. • **Edit**: Displays an editable version of the spreadsheet, allowing you to make and save changes. The Oracle SDM Cloud validates any values added or updated before updating the spreadsheet. • **Set Columns**: Set the columns to be displayed in this table.
Refresh icon	Refresh the contents of the table.

Edit a Spreadsheet

From the Offline Configuration Spreadsheets page, you can select a spreadsheet to edit.

> **Note**
>
> Once a Work Order has begun, the offline configuration is locked and cannot be edited. Once the Work Order is in the Committed state, the lock is released.

1. On the **Configuration Manager** slider, select **Configuration Tools**, **Offline Configuration**.
   The **Offline Configuration** page displays.
2. Click the **Spreadsheets** tab.
   The **Offline Configuration Spreadsheets** page displays.

3. Select the spreadsheet to edit, click the **More Actions** icon, and select **Edit**.
   A list of all devices on the spreadsheet displays.
4. Update any values required and either click **Apply** to save the changes and return to the **Spreadsheets** page or click **Cancel** to discard your changes and return to the **Spreadsheets** page.

Load an Offline Configuration

Use this task to configure, modify, and edit parameters for your offline configuration for your system domain. Note that users cannot load a golden configuration. If a user selects a golden configuration, the **Load** button becomes disabled.

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

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

Search For Golden and Offline Configurations

Users can search for a golden or offline configuration based on specific criteria.

1. Expand the **Configuration Manager** slider and click to expand the **Configuration Tools** folder in the navigation pane.
2. Click **Golden/Offline Configurations**.
3. In the **Golden/Offline Configuration** tab, click **Search**.
   The **Search** dialog box displays.
4. Complete any of the following fields:

Name field	The unique name of the configuration.
Configuration type drop-down list	The type of configuration; either **Golden** or **Offline**.
Product drop-down list	The product with which the configuration is associated.
Software version drop-down list	The software version of the configuration.
Platform drop-down list	The platform with which the configuration is associated.
Created from/to calendars	A date range in which the configuration was created.

5. Click **Apply**.
   The search results display in the Golden/Offline Configuration table. To clear the search results, click **Show All**.

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.

1. On the **Configuration Manager** slider, select **Configuration tools**, **Offline configurations**.
2. Load the offline configuration.
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, click the **More Actions** icon, and select **Edit**.
3. In the **Edit offline configuration** screen, enter the description that you want for this offline configuration.

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

4. Click **OK**.

Manage Configuration Comparison Reports

Through the use of golden configurations, Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) users can compare multiple configurations to generate, save, and download comparison reports.

Comparisons are performed between one source and one target at a time and the component type for each must match. Once a user enters all of the required input and clicks **Apply**, the configuration comparison occurs and the Oracle SDM Cloud displays a progress bar for 15 seconds. If a comparison report is generated and available in that time, the **View Comparison Reports** screen displays the report. If the report takes longer than 15 seconds to generate, the message "The comparison is taking a longer time, please refresh the temporary reports to check the report status after some time" displays and users are redirected to the **Temporary Reports** tab. Click the **Refresh** button to view the status of the comparison report.

The **Configuration Comparison Reports** page contains two tabs, **Temporary Reports** and **Saved Reports**. The **Temporary Reports** page contains reports generated after a comparison. By default, these are saved and viewable for 24 hours before they are deleted. Users can save reports they do not want deleted.

> **Note**
>
> If the Source Host or Target Host columns reference a device, users are able to see only the reports to which the user has device access. However, if there is no device reference, the report is visible to all users who have created or updated the reports.

1. Expand the **Configuration Manager** slider and select **Configuration Tools**, **Golden/ Offline Configurations**.
   The **Config Comparison Reports** table displays by default in the **Temporary Reports** tab, with the following columns:

Report Name	The unique name of the comparison report.
Source GC Name	The name of the golden configuration used for comparison.
Source Seeding Type	The source from which the golden configuration is derived.
Target Seeding Type	The source from which the target configuration is derived.
Product Type	The product type of the configurations.
Source Platform	The golden configuration's platform.
Target Platform	The target configuration's platform.
Source Software Version	The golden configuration's software version.
Target Software Version	The target configuration's software version.
Created Date	The date this comparison report was created.
Report Status	The status of the comparison report.
Source Host Name	The golden configuration's host name.
Source Host IP	The golden configuration's IP address.
Target Host Name	The target configuration's host name.
Target Host IP	The target configuration's IP address.

The **Config Comparison Reports**, **Temporary Reports** page contains the following buttons, fields, and icons:

Add button	Create a new configuration comparison report.
View button	View the selected configuration comparison report.
Save button	Allows the user to provide a unique name and save the configuration comparison report. The saved report then displays in the Saved Reports table.

Search field	Enter the name of a column in the table to search for a specific report.
Refresh icon	Refreshes the table's contents.

Manage Saved Configuration Comparison Reports

The **Saved Reports** tab on the **Config Comparison Report** page allows you to view, search, download, and delete saved configuration comparison reports.

The Saved Reports tab page contains the following buttons, icons, and fields:

View button	Displays the configuration comparison report on the screen.
Delete button	Deletes the selected configuration comparison report. Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) displays a confirmation dialog box. Select **Yes** to delete the report.
Save To File field	Export the selected configuration Comparison Report to a local machine in either PDF or compressed zip format.
Search field	Search for a report by entering any of the column values in the table.
Refresh icon	Refreshes the table's contents.

Create a Configuration Comparison Report

1. On the **Configuration Manager** slider, select **Configuration Comparison**.
   The **Config Comparison Reports** page displays.
2. In the **Temporary Reports** tab, click **Add**.
   The **Create Comparison Report** page displays.
3. Complete the following fields:

Report Name field	Enter a unique name for the report with the following restrictions: • Must start with an alphabetical character • Contain no more than 50 characters • Contain only letters, numbers, underscore, hyphen, or whitespace.
Source Type drop-down list	The source type used for comparison. By default, this value is set to the golden configuration and the drop-down is disabled.
Target Type drop-down list	The target type that is used for comparison. Possible values are: • Managed Device

	• Device Configuration File • Archived Configuration • Offline Configuration
Component drop-down list	Select the component of the source and target to be compared. Only configurations with the same component type can be compared.
Source Device browse icon	Select the device associated with the golden configuration. If a **Component** has been selected, this list displays all devices with the same **Component**.
Select Source browse icon	Provides a list of all golden configurations that match the specified criteria to choose from.
Select Target browse icon	Provides a list of all golden configurations that match the specified criteria to choose from. When Device configuration file is the target type, the user is prompted to upload a data doc as a target for comparison. When Offline configuration is the target type, the users selects the target offline configuration and can choose whether or not to select a spreadsheet or device to associate with the offline config.

4. Click **Apply**.

View and Save Configuration Comparison Reports

Users can view and save generated configuration comparison reports. Comparison reports are displayed in side-by-side panes, highlighting the differences.

1. On the **Configuration Manager** slider, select **Configuration Comparison**.
   The **Config Comparison Reports** table displays.
2. Select the comparison report you want to view and click **View**.
   The **Config Comparison Report** displays the following information:

Source platform	The golden configuration's platform.
Target platform	The target configuration's platform.
Plugin type	The type of plugin used in both configurations.
Source configuration	The golden configuration's name.
Target configuration	The target configuration's name.
Source software version	The golden configuration's software version.

Target software version	The target configuration's software version.
Source host name	The golden configuration's host name.
Source host IP	The golden configuration's IP address.
Target host name	The target configuration's host name.
Target host IP	The target configuration's IP address.
Report generated time	The date and time that this report was created.

3. Close the Comparison Report.
   The **Temporary Reports** page displays.
4. Select a comparison report and click **Save** to save a report.
   The **Config Comparison Report** now displays in the **Saved Reports** table and is not deleted by the Oracle SDM Cloud after 24 hours.

> **Note**
>
> Reports larger than 20MB must be downloaded using a compressed format. If a report is too large, a message displays stating "The Comparison report is too large to view. Please save and download the compressed file.
> Larger comparison reports occur when one or both configurations has a large number of configuration elements.

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.

Users are able to view only the archives associated to devices to which they have access. For more information, see "Apply or Change User Group Privileges" in the *Security Manager* chapter.

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

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.

> **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 **Configuration 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: • **Daily**—Select to perform daily backups. • **Weekly**—Select to perform weekly backups. • **Monthly**—Select to perform monthly backups.
Start Date Time drop-down list	Select a start date using the calendar icon and 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 or which you want to schedule a backup.
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.

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, click the **More Actions** icon and select **Set Columns** to choose the columns that display in this table. The following table describes all of the columns available to view:

Parent Group	The parent network function (NF) group that is provided by the user or Oracle SDM Cloud 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.
Hardware 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.
Device Group	(Hidden) The name of the device group.
Target Name	(Hidden) The target name of the backup.
Source ID	(Hidden) The Source ID of the device group that needs to be archived.
IP Address	(Hidden) The IP address of the device group that needs to be archived.

Export a Configuration From the Configuration Archive

The Oracle® Session Delivery Management Cloud allows you to export an archived configuration from the Configuration Archive to view locally.

1. On the **Configuration Manager** slider, select **Configuration Archive**, **Archived Configurations**.
2. Select the archived configuration to export, click the **More Actions** icon, and select **Export Config**.
   A confirmation banner displays confirming the export, or reporting an error.

   Once you have exported the configuration, you are able to view it.

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**, **Archived Configurations**.
2. Select a backed up configuration from the table, and click **Restore**.

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 **Configuration Archive** folder in the navigation pane.
2. In the navigation pane, click **Archived Configurations**.
3. In the Config Archive - Backups 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	Click the calendar icon to select the end date range for when a configuration was backed up to the configuration archive.

The archive that matches your search appears.

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 the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

> **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 **Configuration Archive**, **Archived Configurations**.
2. In the **Config Archive - Backups** pane, select the configuration you want to rename, click the **More Actions** icon and select **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.

Create a Configuration Purge Policy

A purge policy must be selected and configured to have Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) automatically delete configurations. You can also manage backed up configurations manually.

The Oracle SDM Cloud service provides the archive configuration name prefix for the archive configuration file name. The archived configuration files are kept in the Oracle SDM Cloud server folder name ConfigBackups under the AcmePacket directory. The archived configuration file for each device uses the device IP address in the directory path.

> **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 **Configuration Archive**, **Administration**.
2. On the **Purge policy** page, specify the **Interval in Number of Backups Per Device** value.
3. Click **Apply**.

6
Fault Manager

Fault Management system allows you to manage all events, notifications, and alerts generated by either Networks Function (NF) or Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) components. For the Session Border Controller (SBC), Enterprise Session Border Controller (E-SBC), and Oracle Communications Session Monitor (OCSM), the Events and Alarm information is based on the Oracle® standard and proprietary Management Information Bases (MIBs). All SNMP traps generated from these NFs are managed by Oracle SDM Cloud. The NFs send their traps to the Management Cloud Engine (MCE) located on the customer premises which acts as the trap receiver. The MCE then converts the SNMP trap into a REST payload which it sends to the cloud Oracle SDM Cloud SaaS offering. For more information on configuring traps, refer to the appropriate configuration user guide for that product.

- For SBC related products, see SBC documentation: https://docs.oracle.com/en/industries/communications/session-border-controller/index.html
- For E-SBC related products, see E-SBC documentation: https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/index.html
- For Oracle Communications Session Monitor (OCSM), currently Configuration Manager does not support Mediation Engine configuration. For information on configuring the OCSM, see https://docs.oracle.com/en/industries/communications/session-monitor/index.html

The Fault Manager provides views for events and alarms.

- **Events view**—Provides a historical view of all events generated by either managed NFs or by Oracle SDM Cloud components. This allows you to track the time and state of when NF traps of Oracle SDM Cloud alerts entered the system and how, for a specific failed resource, the associated events transitions to different states on a row per row basis.
- **Alarm view**—Provides a summary view of the latest state of an alarm for a specific failed resource. This table provides only one row for each unique failed resource and updates this row with the latest information as new events for the same failed resource are identified.

For example, consider that "SBC-1" sends a **apSysMgmtFanTrap** trap which crosses the following states:

- Fan speed Trap Minor alert: fan speed is more than minor alarm threshold, but less than major alarm threshold.
- Fan speed Trap Major alert: fan speed is more than major alarm threshold, but less than critical alarm threshold.
- Fan speed Trap Critical alert: the environment is very bad, such as Fan speed is more than critical threshold.

The Events view displays 3 events in the table for the failed resource Fan for device "SBC-1".

```
Event 1 Fan speed Minor alert event at Time.0.
Event 2 Fan speed Major alert event at Time.1.
Event 3 Fan speed Critical alert event at Time.2.
```

The Alarms view displays only 1 row for the failed resource, displaying only the most current state.

```
Event 1 Fan speed Critical alarm at Time.2.
```

The following pre-requisites are required for receiving fault notifications:

- You must use the sudo password (the password of the NNCentral user account on the server operating system) for the port on which TrapRelay listens. This port is configured during Media Cloud Engine (MCE) installation. For more information, see the *Getting Started* guide.

  > **Note**
  >
  > If you use port 1024 for the TrapRelay function, root permission is not required.

- Ensure that SNMP communities and the MIB administrator contact name is configured on your southbound system(s).
- A trap receiver for each MCE node in a cluster must be configured on each southbound device. Also, the SNMP community defined in the trap receiver must be the same for all MCE cluster nodes.

Alarm and Event Configuration Tasks

The following sections describe the **Events** table and **Alarms** table, with their accompanying features. The **Events** table shows a one to one correspondence with all device traps and generated server events. The **Events** table maintains the precise history of all events created and recorded. The **Alarms** table summarizes the **Events** table by showing the most recent update for the specific categories, failed resources, state and devices in each row.

> **Note**
>
> Users can view only the alarms and events for the devices to which they have access, however, events and alarms generated by Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) itself are accessible to all users.

Manage How Events are Displayed

1. Expand the **Fault Manager** slider and select **Events**.
2. Click the **More Actions** icon and select **Set Columns** to choose which columns are displayed in the Events table. The following table describes all of the columns available to view.

Time	The date and time this event was generated in hours, minutes, and seconds.
Source	The exact descriptive source of the event.
Source IP	The IP address from which this event was generated.

Severity	One of the following user-defined severity levels can display for a system event: **Note** The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green.

	• (9) DETAIL—Detailed messages appear. The default color is lime green.
Category	The type of trap associated with this event. For example, TrapRelayMonitor.
Trap Name	The exact name of the trap associated with this event. For example, apNNCTrapRelayAliveNotification.
Failed Resource	The resource responsible for this event.
Description	A short description of the event.
Source Group ID	The identity of the source group associated with this event.
Network Function	The network function associated with this event.

3. In the events pane, select an event that you want to view, click the **More Actions** icon and select **View**.
4. In the **Event detail** dialog box, view the following fields for this specific event:
   - Time Created
   - Description
   - Severity
   - Default Severity
   - Source
   - Source IP
   - Failed Resource
   - Category
   - Trap Name
   - System Up Time
   - Type

Manage How Alarms are Displayed

1. Expand the **Fault Manager** slider and select **Alarms**.
2. Click the **More Actions** icon and select **Set Columns** to choose which columns are displayed in the Alarms table. The following table describes all of the columns available to view.

Time	The date and time this alarm was generated in hours, minutes, and seconds.
Source	The exact descriptive source of the alarm.
Source IP	The IP address from which this alarm was generated.
Severity	One of the following user-defined severity levels can display for a system alarm:

	Note The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green. • (9) DETAIL—Detailed messages appear. The default color is lime green.
Category	The type of trap associated with this alarm.
Acknowledged by	The user that acknowledged the alarm.
Trap Name	The exact name of the trap associated with this alarm. For example, apNNCTrapRelayAliveNotification.
Failed resource	The resource responsible for this alarm.
Description	A short description of the alarm.
Annotation	The user-defined note pertaining to this alarm.
Source Group ID	The identity of the source group associated with this alarm.
Network function	The network function associated with this alarm.

3. In the alarms pane, select an alarm that you want to view, click the **More Actions** icon and select **View**.
4. In the **Alarm detail** dialog box, view the following fields for this specific alarm:
   - Annotation
   - Acknowledged by
   - Time
   - Description
   - Severity
   - Source
   - Source IP
   - Failed Resource
   - Category
   - System Up Time
   - Trap Name
   - Type

Manage the Page View for Events

1. Expand the **Fault Manager** slider and select **Events**.
2. In the Events pane, you can select from the following actions:

Refresh button	Click to refresh the data.
Show all button	Click to show all current events.

Oracle SDM Cloud Alarm Auto Refresh

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms pane, you can select from the following actions:

Auto Refresh button	Click to set a time, in seconds, that the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) automatically refreshes the data in the Alarms table. The default value is 15 seconds and the maximum value allowed is 3600 seconds. When you set this field and click **OK**, a **Stop Auto Refresh** button appears, allowing you to cancel the auto refresh functionality at any time.

	Note When you navigate away from the Alarms page, the auto refresh functionality is canceled.
Show all button	Click to show all current events.

Search for Alarms or Events by Specifying a Criteria

You can search for events and alarms by specifying one, some, or all of the search selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events pane, click **Search**.
3. In the **Search** dialog box, complete the following fields:

Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note** The date you select ends at 11:59:59 PM.
Source field	The source name for this device.
Source IP field	The IP address for this source device.
Trap name drop-down list	Select the trap name (applies to events only).
Category	Select the Category of Event or Alarm. Valid values are as follows: • Voltage change

	• CRL retrieval failure • DIAMETER Server • CPU load • Media port utilization • Task • System Mgmt Database Reg Cache Capacity • Realm Icmp Failure • Core Load Balancer • RADIUS Servers • ThreadUsageOverload • H248 port map usage • Diameter director connection • ACLDrop
Severity drop-down list	Select the severity level for this alarm.
Type drop-down list	Select the alarm type.

Save Alarms or Event Data to a File

You can save event or alarm data in the content area to a comma-separated values (CSV) file that stores table data (numbers and text) in plain-text form.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. Click **Save to file**.

> **Note**
>
> The files are saved to your browser's default download location. Only the first 1000 entries can be saved to file.

Delete Alarms or Events

The appropriate administrator privileges must be assigned to delete alarms or events.

> **Note**
>
> Deleting an alarm in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) has no affect on the node because the node is unaware that Oracle SDM Cloud displayed the alarm or deleted it from the alarms table.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events table, click the alarm or event that you want to remove, click the **More Actions** icon, and select **Delete**.
3. In the **Delete** dialog box, click **Yes** to confirm the deletion of the alarm or event.

Specify a Criteria to Delete Alarms and Events

The appropriate administrator privileges must be assigned to delete alarms or events.

Use this task to specify one or more criterion for deleting alarms or events from Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the events or alarms pane, click the **More Actions** icon, and select **Delete by criteria**.
3. In the **Search** dialog box, complete the following fields:

> **Note**
>
> When there is a high number of faults that are being sent from devices, a purge interval of 2 days for events and 7 days for alarms is suggested.

Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note** The date you select ends at 11:59:59 PM.
Source field	The source name for this device.
Source IP field	The IP address for this source device.
Trap Name drop-down list	Select a trap name.

	Note **Trap Name** is only available for Events and not Alarms.
Category drop-down list	Select a category.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm or event.

4. Click **OK**.

Alarm Specific Configuration Tasks

Alarms play a significant role in determining the overall health of the system. An alarm is triggered when a condition or event happens within the hardware or software of a system (node). Alarms contain an alarm code, a severity level, a textual description of the event, and the time the event occurred. The following sections describe how to configure the way alarms display in Oracle® Session Delivery Management Cloud.

Add an Annotation to an Alarm

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, click the alarm to which you want to add explanatory note, click the **More Actions** icon, and select **Edit**.
3. In the Edit annotation dialog box, add your explanatory note about this alarm in the **Annotation** field.
4. Click **OK**.

Enable Alarm Acknowledgment

The appropriate administrator privileges must be assigned to acknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to acknowledge and click **Acknowledge**.
3. In the **Acknowledge** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.
5. Click the alarm to view an updated **Alarm detail** dialog box with the **Acknowledged by** and **Last modified** fields updated.
6. Click **OK**.

Disable Alarm Acknowledgment

The appropriate administrator privileges must be assigned to unacknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.

2. In the alarms table, select the alarm that you want to unacknowledge and click **Unacknowledge**. The Acknowledge dialog box appears.
3. In the **Unacknowledge** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.

Clear an Alarm

The appropriate administrator privileges must be assigned to clear alarms.

> **Note**
>
> Clearing an alarm in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud)has no affect on the node because the node is unaware that Oracle SDM Cloud displayed the alarm or changed its severity to clear.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to clear, click the **More Actions** icon, and select **Clear**.
3. In the **Clear** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.

Customize Trap Severity Levels

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. In the **Trap Event Setting** page, select the alarm trap groups you are customizing from the **Trap Groups** table:

   > **Note**
   >
   > The Oracle SDM Cloud determines the trap groups that you can access.

3. Select a trap from the **Trap OIDs** table.
4. In the **Severity Mapping** table, select a severity cell from the **Current severity** column for a trap condition row that you want to modify.
5. In the drop-down list of severity levels that appears, click the severity level that you want to apply.

   > **Note**
   >
   > The **Default severity** column serves as a reference point and continues to show the default severity setting for the trap condition.

   The new level appears in the **Current Severity** column for the trap condition.
6. Click **Apply**.
7. In the success dialog box, click **OK**.

Customize Product Plugin Event Traps

The trap event setting allows you to override the default severities and customize them. Traps groups are provided for each product plugin that is installed in Oracle SDM Cloud. When you select a trap group the product plugin, SNMP trap (OID) list is provided. For more information on product-specific traps, refer to the appropriate MIB Reference Guide.

- For SBC related products, see SBC documentation: https://docs.oracle.com/en/industries/communications/session-border-controller/index.html
- For E-SBC related products, see E-SBC documentation: https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/index.html
- For OCSM related products, see OCSM documentation: https://docs.oracle.com/en/industries/communications/session-monitor/index.html

See your element manager product plugin documentation for the list of SNMP event traps and their definitions.

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. Select a trap group row from the **Trap groups** table and click **OK**.

Customize Session Delivery Manager Event Traps

The trap event setting allows you to override the core Oracle SDM Cloud default event trap severities and customize them.

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. In the **Select** dialog box, select the **SDM** trap group row from the **Trap groups** table and click **OK**.
3. The following table describes the Oracle SDM Cloud product event types and a description that references its respective trap.

Trap	Description
apUmsNodeUnreachable	The trap is generated when the status of a node changes from reachable to unreachable. The trap contains the node ID of the device and the time of the event.
apUmsNodeUnreachableClear	The trap is generated when the status of a node changes from unreachable to reachable. The trap contains the node ID of the device and the time of the event.
apUmsRegistration	The trap is generated when, upon startup, the MCE successfully registers with Oracle SDM Cloud automatically.
apUmsMCERegistrationClear	The trap is generated when, after an unsuccessful registration attempt, the MCE is able to register with Oracle SDM Cloud successfully.
apUmsServiceStarted	When the Oracle SDM Cloud starts and initializes each of its sub-services, this trap displays the status of each sub-service.

Trap	Description
apUmsONSThrottling	When email notifications are temporarily suspended, as the OCI Notification Service is unable to deliver messages.
apUmsONSThrottlingClear	The trap generated when the OCI Notification Service is able to deliver messages again.
apUmsDBUsage	When the DB usage crosses the threshold value: • WARNING - Total DB utilization (default + optional) across > 80% and < 85% • MAJOR - Total DB utilization (default + optional) across >= 85% and < 90% • CRITICAL - Total DB utilization (default + optional) across >= 90%
apUmsDBUsageClear	When DB usage returns to < 80%.
apUmsInvalidMCERegistration	When an MCE tries to connect to a site using invalid registration ID or when an MCE tries to connect to a site which already has a MCE connection.
apUmsTestTrap	Checks the connectivity to a specific trap receiver.

Search on Trap OIDs

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports searching on Trap OIDs to find specific traps.

To search for traps using Trap OIDs:

1. Expand the **Fault Manager** slider and click **Trap Event Settings**.
   The Trap Event Settings page displays.
2. **Trap Groups**—Select the Trap Group in which you want to search.
3. **Trap OIDs**—Enter the Trap OID you want to search on. As you start to type, the **Trap Descriptor** list shows all matches which contain the typed string.
4. **Trap Descriptor**—Select the Trap you are searching on.
   The trap displays in the Severity Mapping table.

Manage Trap Receivers

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports trap forwarding to northbound trap receivers using the Management Cloud Engine (MCE) for local trap forwarding of traps generated by NFs managed by Oracle SDM Cloud and the Oracle SDM Cloud itself in the ITUX.733 format and Pass through (the same format as generated by the NF itself).

To enable this functionality, users must configure trap receivers and trap filters, then create trap forwarding maps.

The Trap Receivers page displays a table with a list of all trap receivers configured on the Oracle SDM Cloud. Users can add, edit, delete, refresh the list, and synchronize traps.

The Trap Receivers table displays the following information:

IP Address/FQDN	The trap receiver's IP Address or FQDN.

SNMP Version	The trap receiver's SNMP Version, either **SNMPv2** or **SNMPv3**.
SNMP Port	The trap receiver's SNMP port number.
User Name	The name of the user who created this trap receiver.
Authentication Protocol	The trap receiver's authentication protocol, either **HMAC192SHA2256**, **HMAC384SHA5126**, or **None**.
Privacy Protocol	The trap receiver's privacy protocol, either **AES128** or **None**.
Trap Pass Through	Specifies whether trap pass through is enabled for this trap receiver. When **Yes** is selected, the Oracle SDM Cloud forwards the traps generated from NFs without any changes to the trap receiver. When **No** is selected, the traps generated from NFs are forwarded in ITUX.733 format.
Community String	The trap receiver's configured community string.

The Trap Receivers page contains the following buttons:

Add button	Add a new trap receiver. Clicking this button opens the Add Trap Receiver page.
Edit button	Select a trap receiver from the list that you want to update and click **Edit**.
Delete button	Deletes the selected trap receiver.
Synchronize button	Synchronizes the traps between Oracle SDM Cloud and the selected trap receivers.
Refresh icon	Refreshes the Trap Receivers table.

Add a Trap Receiver

To add a trap receiver:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Receivers**.
   The Trap Receivers page displays.
2. Click **+Add**.
   The Add Trap Receiver page displays.
3. Complete the following fields:

IP Address/FQDN field	Enter either the IP address or FQDN of the trap receiver. The value entered must be unique and must be valid and is validated by the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) When an invalid

	or already used value is entered, Oracle SDM Cloud returns an error.
SNMP Version drop-down list	Select the SNMP version. Valid values are: • SNMPv2 (default) • SNMPv3
SNMP Port field	The SNMP port to use for this trap receiver. The default value is **162**.
Community String field	(Only displays when **SNMP Version** is set to **SNMPv2**) Enter a community string to be used for this trap receiver.
User Name field	(Only displays when **SNMP Version** is set to **SNMPv3**) Enter a user name for this trap receiver.
Authentication Protocol drop-down list	(Only displays when **SNMP Version** is set to **SNMPv3**) Select the authentication protocol to use. Valid values are: • None (default) • HMAC192SHA2256 • HMAC384SHA5126
Authentication Password field	(Only displays when **SNMP Version** is set to **SNMPv3**) When **Authentication Protocol** is set to a value other than **None**, enter a password to use. The minimum password length is 6 characters and the maximum length is 15.
Privacy Protocol drop-down list	(Only displays when **SNMP Version** is set to **SNMPv3**) When **Authentication Protocol** is set to a value other than **None**, select the privacy protocol to use. Valid values are: • AES128 • None (default)
Privacy Password field	(Only displays when **SNMP Version** is set to **SNMPv3**) When **Privacy Protocol** is set to a value other than **None** enter a password to use. The minimum password length is 6 characters and the maximum length is 15.
Trap Pass Through drop-down list	Select **Yes** to enable trap pass through or select **No** to disable the feature.

4. Click **Apply** to create the trap receiver or **Cancel** to discard your inputs and return to the Trap Receiver screen.
The newly created trap receiver displays in the Trap Receiver table.

Edit a Trap Receiver

To edit a trap receiver:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Receivers**.
   The Trap Receivers page displays.
2. Select the trap receiver you want to edit by checking its checkbox and click **Edit**.
3. Update the trap receiver as necessary.
4. Click **Apply** to save your changes or **Cancel** to discard the changes and return to the Trap Receiver screen.

Delete a Trap Receiver

To delete a trap receiver:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Receivers**.
   The Trap Receivers page displays.
2. Select the trap receiver(s) you want to delete by checking its checkbox and click **Delete**.
   A confirmation pop-up displays.
3. Click **Yes** to delete the trap receiver or **No** to cancel.

Synchronize Trap Receivers

The Synchronization feature allows users to synchronize the traps between Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) and trap receivers.

Only one trap receiver can be synchronized at a time and the Synchronize button is disabled when either no trap receiver is selected or more than one trap receiver is selected.

To synchronize a trap receiver:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Receivers**.
   The Trap Receivers page displays.
2. Select the trap receiver you want to synchronize by checking its checkbox and click **Synchronize**.
   The Trap Synchronization dialog box displays.
3. Enter values for the following fields:

Synchronize from radio buttons	Select either **Alarms** or **Events**.
Synchronization filters drop-down list and **Preview** icon	Select a trap filter from the drop-down list. This list contains all of the trap filters configured on the Oracle SDM Cloud whether they are enabled or disabled. Once you select a filter, click the **Preview** icon to view the selected filter.
Start Time calendar	Select a start time for the trap receiver.
End Time calendar	Select an end time for the trap receiver. This value must be greater than the **Start Time**.

4. Click **Apply** to synchronize the traps or **Cancel** to quit the action.

When a user clicks **Apply**, either the traps from events or alarms in the Oracle SDM Cloud, filtered based on the criteria specified, are sent to the Management Cloud Engine (MCE). The MCE then forwards these traps to the trap receiver. If the selected trap receiver is associated with multiple MCEs, the filtered traps are sent only to one MCE.

The trap filter Preview displays the details of the trap filter selected, as follows:

- If the selected trap filter has a trap name, the preview displays:
  - Filter Name
  - Trap Name
  - Forward Clear Trap association
- If the selected trap filter has trap severity, the preview displays:
  - Filter Name
  - Trap Severity
  - Forward Clear Trap association
- If the selected trap filter has trap source, the preview displays:
  - Filter Name
  - Trap Source
  - Suppress Forwarding Option (true/false)
  - Forward Clear Trap association

Manage Trap Filters

The Trap Filters page displays a table with a list of all trap filters configured on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud). Users can add, edit, delete, and refresh trap filters.

The Trap Filters table displays the following information:

Name	The unique name of this trap filter.
Trap Severity	The severity level of this trap filter.
Trap Name	The trap name associated with this filter.
Trap Source	The IP Address or FQDN
Suppress Forwarding	Specifies whether suppress forwarding is enabled or disabled on this trap filter.
Forward Clear Trap	Specifies whether forward clear trap is enabled or disabled on this trap filter.

The Trap Filters page contains the following buttons:

Add button	Add a new trap filter. Clicking this button opens the Add Trap Filter page.
Edit button	Select the trap filter from the list that you want to update and click **Edit**.
Delete button	Deletes the selected trap filter.

Refresh icon	Refreshes the Trap Filters table.

Add a Trap Filter

Users can create up to 100 trap filters.

To add a trap filter:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Filters**.
   The Trap Filters page displays.
2. Click **+Add**.
   The Add Trap Filters page displays.
3. Complete the following fields:

> **Note**
>
> You must choose to use either Trap Name, Trap Severity, or Trap Source to add a trap filter. Once a value is added to one of those parameters, the other two are disabled.

Filter Name field	The unique name for this filter that adheres to the following rules: • A minimum length of 3 and a maximum length of 50 characters. • Only containing letters, numbers, underscore (_), hyphen (-), or whitespace. • Must start with a letter.
Trap Name drop-down list	Select a trap name from the list. This field is enabled only when there are no values selected for **Trap Severity** and **Trap Source**.
Trap Severity drop-down list	Select the trap severity from the list. This field is enabled only when there are no values selected for **Trap Name** and **Trap Source**. When the filter criteria is **Trap Severity** for all traps received by the UMS, the overridden severity is used for filtering. For the ITUX.733 format, this severity value is converted to either: • Unknown • Clear • Indeterminate • Critical

	• Major • Minor • Warning
Trap Source field	Enter the trap source device's FQDN or IP address or Oracle SDM Cloud to filter the traps generated by Oracle SDM Cloud. This field is enabled only when there are no values selected for Trap Name and Trap Severity.
Suppress Forwarding checkbox	When a value is configured for **Trap Source** , enable or disable Suppress Forwarding. By default this value is disabled. When this value is enabled, **Forward Clear Trap** is automatically disabled.
Forward Clear Trap checkbox	Enable or disable forwarding a clear trap. When **Suppress Forwarding** is enabled, this field is automatically disabled.

4. Click **Apply** to create the trap filter or **Cancel** to discard your inputs and return to the Trap Filter screen.
   The newly created trap filter displays in the Trap Filter table.

Edit a Trap Filter

To edit a trap filter:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Filters**.
   The Trap Filters page displays.
2. Select the trap filter you want to edit by checking its checkbox and click **Edit**.
3. Update the trap filter as necessary.
4. Click **Apply** to save your changes or **Cancel** to discard the changes and return to the Trap Filter screen.

Delete a Trap Filter

To delete a trap filter:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Filters**.
   The Trap Filters page displays.
2. Select the trap filter(s) you want to delete by checking its checkbox and click **Delete**.
   A confirmation pop-up displays.
3. Click **Yes** to delete the trap filter or **No** to cancel.

Manage Trap Forwarding Maps

The Trap Forwarding Map page displays the association of Management Cloud Engines (MCE) with the trap receivers and trap filters, allowing users to view, create, and enable new trap receiver and trap filter mappings with MCEs.

The Trap Forwarding Map page contains two tables, the first showing the Association of MCE with trap receivers and the second showing the Association of MCE with trap filters. Both tables contain the following columns:

Enable/Disable	Specifies the status of the map.
Map	The name of the map.

This page contains the following fields and buttons:

+ Associate button	Allows users to associate MCEs with trap receivers and trap filters.
Refresh icon	Refreshes the Trap Forwarding Map tables.
Association of MCE with trap receivers Search field	Search within the MCE trap receiver associations.
Association of MCE with trap receivers Expand All/Collapse All icon	Expands and collapses the table. When the table is expanded, the **Collapse All** icon is enabled and when the table is collapsed, the **Expand All** icon is enabled.
Association of MCE with trap receivers Enable/Disable checkbox	Enable the association by checking the checkbox and disable the association by unchecking the checkbox.
Association of MCE with trap filters Search field	Search within the MCE trap filter associations.
Association of MCE with trap filters Expand All/Collapse All icon	Expands and collapses the table. When the table is expanded, the **Collapse All** icon is enabled and when the table is collapsed, the **Expand All** icon is enabled.
Association of MCE with trap filters Enable/Disable checkbox	Enable the association by checking the checkbox and disable the association by unchecking the checkbox.
Save button	Saves any enable or disable actions a user has made.
Cancel button	Undo any unsaved changes.

Enable or Disable Trap Forwarding

To enable or disable trap forwarding:

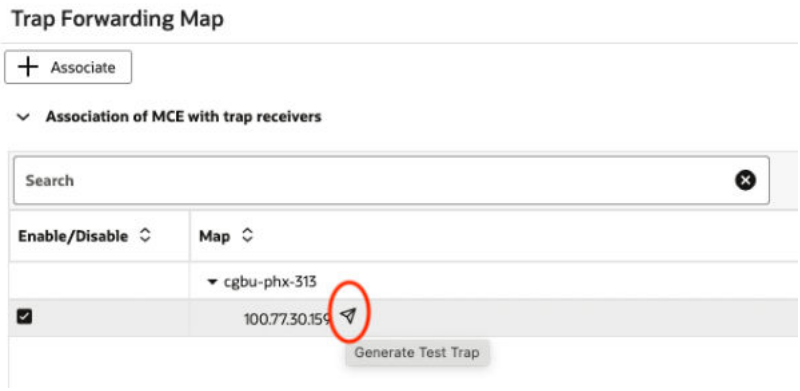
1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Forwarding Map**. The Trap Forwarding Map page displays.
2. Browse to the map(s) you want to enable or disable and check or uncheck the checkbox.
3. Click **Save** to save your updates or **Cancel** to undo any unsaved changes.

Generate a Test Trap

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides users a way to generate a test trap, ensuring a trap is configured properly.

To generate a test trap:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Forwarding Map**.
   The Trap Forwarding Map page displays.
2. Browse to the trap receiver you want to test and click the **Generate Test Trap** icon next to the IP address/FQDN (the icon cirlced in red below).



   A Confirmation dialog box displays.
3. Click **Yes** to continue to generate a test trap or **No** to cancel the action.
   The Oracle SDM Cloud provides either a Success or Error message.
4. Browse to **Fault Manager**, **Events** to see details about the test trap.

Associate Trap Receivers and Trap Filters

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides a two step process for users to associate trap receivers and trap filters, first selecting the Management Cloud Engine(s) (MCE), then selecting the trap receivers and trap filters with which to associate.

To associate trap receivers and trap filters:

1. Expand the **Fault Manager** slider and select **Trap Forwarding**, **Trap Forwarding Map**.
   The Trap Forwarding Map page displays.
2. Click **Associate**.
   The Select MCEs page displays, listing all of the MCEs available.
3. Select the MCE(s) to use for the association.
4. Click **Next**.
   A confirmation dialog displays explaining that if you continue, any existing associations for the selected MCEs will be removed and the new associations will be applied to all MCEs in cross-site with them.
5. Click **Yes** to continue or **No** to cancel the action.
   If you continue, the Trap Receivers & Filters page displays, showing all available trap receivers and trap filters.
6. Select the trap receivers to associate with the MCE(s).

> **Note**
>
> A maximum of 3 trap receivers can be selected.

7. Select the trap filters to associate with the MCE(s).

> **Note**
>
> A maximum of 50 trap filters can be selected.

8. Click **Finish** to save the mappings.
   The Trap Forwarding Map displays showing the updated mappings. By default all of the trap receivers and trap filters associated with the MCE are enabled.

   When users assign a site with an MCE to a site with another MCE, the trap receiver and trap filter mappings are applied for all MCEs associated with the site.

7

Work Order Manager

Work Order Manager allows you to create, edit, delete and manage all work orders on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

The Work Order Administration Manager page contains the Work Order Administration table, containing a list of all work orders created, running, and completed in the Oracle SDM Cloud. The table displays the following information for each work order:

Name	The work order name.
Type	The work order type. • **NF Upgrade/Downgrade** - Upgrade device software on the targeted devices. • **LRT Update** - Update the LRT on the targeted devices.
Device Count	The number of targeted device nodes affected by the work order. **Note** A HA pair is treated as one device node.
Status	The status of the work order: • **Partially-Configured** - The work order configuration is not completed. • **Ready** - The initial state of the work order when created. • **WaitToStart** - The work order task has been scheduled or the host machine has received the task and it is in queue. • **Running** - The work order is currently being executed. • **Pausing** - A user has requested a running work order to pause. • **Paused** - A running work order has been successfully paused. • **Success** - A work order has been successfully executed.

	• **Failed** - A work order task has failed to be executed. • **Committing** - Either the user requested or upon automatic commit for a work order task that is in its final states. • **Committed** - A work order task has been committed successfully. • **CommitFailed** - A work order failed to be committed. • **StartAbort** - An abort operation has been requested by the user on a work order task. • **Aborting** - A work order is in the middle of an abort operation. • **Aborted** - Work order has been successfully aborted. • **AbortFailed** - Abort operation failed for the work order.
Start Time	If a work order has been scheduled, this column displays the scheduled time. If the work order has already been started, this column contains the actual start time. **Note** The Oracle SDM Cloud displays and stores this time in UTC.
End Time	The time at which the work order paused or stopped, either successfully or when a failed condition is met. **Note** The Oracle SDM Cloud displays and stores this time in UTC.

When adding a new work order, the Oracle SDM Cloud provides a wizard that guides you through the process and at any time during the work order creation process, you can click the **Summary** button. This button displays a dialog providing an overview of the work order thus far.

> **Note**
>
> Users are able to manage work orders only if they have access to all of the components within the work order. When a user does not have access to some of the devices selected in a work order, they are only able to view the work order.
> The following lists the components for different types of work orders:
>
> - LRT Work Order–The user must have access to both the Route sets and the devices that are part of the work order.
> - Device Config Work Order–The user must have access to the Offline Config, Spreadsheet, and associated devices.
> - NF Upgrade/Downgrade–The user must have access to the devices.

The Work Order Administration page contains the following buttons and icons:

+ Add button	Allows you to add a work order. Clicking this button brings you to the Work Order wizard.
Logs button	Displays work order level logging messages for the selected work order. If the task is still running you can click the **Refresh** button to refresh the log. Users can also export the file to a local disk.
Search button	Allows you to search for work orders based on the following criteria: • **Name** - The name of the work order. • **Type** - The type of work order. • **Status** - The status of the work order. The Work Order Administration page displays only the work orders that match the search criteria.
Clear Search button	Deletes the current search and goes back to displaying all configured work orders.
Delete button	Deletes the selected work order from the Oracle SDM Cloud database. A work order can only be deleted if it is in one of the following states: • PartialConfigured • Ready • Commited
More Actions icon	Provides a drop-down list with the following additional actions for a selected work order: • **Pause** - Pauses the selected work order, if the work order is currently running.

	• **Start / Restart /Resume** - Starts, restarts, or resumes a work order depending on the work order state. The label of the button automatically changes based on the work order state. • **Edit/View** - Launches the Edit Work Order Wizard and allows you to edit the selected work order. A work order can only be modified if its state is in PartiallyConfigured or Ready. If the work order cannot be edited, a read-only view of the work order wizard is launched. • **Abort** - Cancels the selected work order, if the work order is currently running and all targeted NFs are rolled back exactly as before the work. • **Commit** - Manually commit a selected work order. • **Copy** - Duplicates a work order configuration, including devices, and puts the work order in the PartialConfigured state. This copy must be modified before the work order can be executed. • **Devices** - Displays the Device Task Table, allowing you to view the progress and status of each device Node task and manage its execution.
Refresh button	Refreshes the list of configured work orders.

Work Order Wizard

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides a wizard, rendering the relevant steps you need to go through to create or edit a work order. The wizard launches when you click **+Add** and select the appropriate work order type.

The wizard contains the following navigation buttons:

Cancel	Ignores any user input and exits the wizard screen.
Back	Navigates to the previous step.
Next	Navigates to the next step.
Summary	Displays a dialog providing an overview of the work order thus far.
Finish	This button is only available at the last step of the wizard. Indicates to the wizard that you are done configuring the work order. The Oracle SDM Cloud runs a validation and if it passes, saves the work order to the database. If it

	fails, the Oracle SDM Cloud displays an error message.

Add NF Upgrade Work Order

Adding an Upgrade work order prompts the **Add NF Upgrade Work Order Wizard** to begin. There are 4 screens in the Wizard:

- **Devices**
- **Settings**
- **Software Images**
- **Work Flow**

To add an Upgrade work order:

1. Expand the **Work Order Manager** slider and select **Administration**.
2. Click **Add**.
   The **Select Work Order Type** dialog appears.
3. Select **NF Upgrade/Downgrade** and click **Apply**.
   The **Add NF Upgrade Work Order Wizard** launches, bringing you to the **Add NF Upgrade Work Order**, **Devices** page.

Devices

The **Add NF Upgrade Work Order**, **Devices** page displays a table containing all device nodes being displayed in Device Manager. This page allows you to select the devices to be serviced by the work order. The table includes the following columns:

Name	The device node name. A device node can signify a standalone device or devices configured as a HA pair.
Version	The current running software image version on the node.
IP Address	The IP address of the device.
Platform	The platform of the device.
Product	The device product (for example, SBC).
Selected	Specifies if the device is targeted to be serviced via this work order.

The following buttons appear on this page:

Clear button	Removes all search criteria and de-selects all devices.
Search button	Create a search of NFs managed by the Oracle SDM Cloud based on specified criteria. You can filter based on the following: • **Device Type (Standalone or HA)** • **Name**

	• **IP Address** • **Version** • **Platform** • **Product** Click **Apply** to create the search or **Cancel** to exit out.
Clear Search button	Clears the table of the results of an existing search, but keeps the selected devices as-is.
Refresh icon	Refreshes the Devices table.
Expand All/ Collapse All icon	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Expand All** icon is enabled.

1. Select the device or HA pair for which you want to create a work order by selecting the checkbox in the **Selected** column.

> **Note**
>
> After the first device or HA pair is selected, the remaining devices in the table are filtered so that only "similar" devices are shown. The Oracle SDM Cloud filters the remaining devices based on the following rules:
>
> - If the first selected device is Standalone, then only Standalone devices are available for selection and the same thing goes for HA pairs.
> - Only devices on the same platform as the first selected device.
> - Only devices running the same major and minor software versions are available for selection.

2. Click **Next**.
   The **Add NF Upgrade Work Order**, **Settings** page displays.

Settings

The **Add NF Upgrade Work Order**, **Settings** page allows you to configure some logistical information about the work order.

1. Enter values for the following parameters:

Work Order Name field	Enter a unique name for this work order. This is a required field and you cannot select Next or move to **Software Images** or **Work Flow** without entering a value here. The following naming conventions apply: • Names can contain only letters, numbers (0-9), or underscores (_). • Names cannot start or end with underscores.

	• Names cannot contain consecutive underscores. • Names cannot contain whitespaces.
Auto Commit checkbox	Specify whether you want to the work order to be automatically committed after it is successfully executed. By default this is disabled. When this feature is off, you must manually commit the work order.
Scheduled Start Time (UTC) checkbox	Specify whether you want to schedule a start time for this work order. When the checkbox is checked, the **Date** field and calendar become enabled. By default this is disabled.
Date/Time calendar	When **Scheduled Start Time (UTC)** is enabled, this calendar widget is enabled. Select the date and time you want to schedule this work order. This value is both displayed and stored in UTC.
Run Device Task Concurrently checkbox	Specify whether you want to upgrade multiple devices concurrently. When this checkbox is selected, the **Behavior** and **Error Policy** parameters are disabled.
Behavior drop-down list	Specify the behavior when upgrading or downgrading multiple devices: • **Never pause** - The work order does not pause after each device is upgraded. This is the default value. • **Pause after every device** - The work order pauses after each device is upgraded. • **Pause only after first device** - Pause after upgrading or downgrading the first device only.
Error Policy drop-down list	Specify how to behave when an error is encountered during the work order: • **Log and proceed** - The device which failed upgrade is rolled back, but the work order continues on the remaining devices. • **Stop** - The device which failed upgrade is rolled back and the work order on the remaining devices is halted. • **Stop and rollback** - The work order stops and any devices that have already been upgraded are rolled back.

Operation Timeout (Min.) drop-down list	Specify how long (in minutes) the Oracle SDM Cloud waits before timing out on a work order. The default value is **15** minutes.

2. Click **Next**.
The **Add NF Upgrade Work Order**, **Software Images** page displays.

> **Note**
>
> The **Add NF Upgrade Work Order**, **Software Images** link is disabled until you select a device on the **Devices** page. If you have not selected a device on the **Devices** page and click **Next** to go to the **Software Images** page, the Oracle SDM Cloud displays the error, **Error: Please select devices**.

Software Images

The **Add NF Upgrade Work Order**, **Software Images** page provides a table listing all software images stored in the repository and allows you to select the software image to which you are upgrading. In addition to the software image, you can also select to upgrade your boot loader image. This table is filtered to show only images that are applicable to the selected NFs.

The table displays the following information for each software image:

Software Image File name	The name of the image file.
Plugin	The type of plugin supported.
Size (Bytes)	The file size, in bytes.
Date/Time created	The date and time the image was created.
Version	The software version.

If the software or boot loader image to which you are upgrading has not been uploaded yet, you can upload it using this page.

This page contains the following buttons and fields:

Refresh button	Refreshes the list of software images stored in the repository.
Add button	Upload a software image to add to the repository.
Select Boot Loader Image checkbox	Select if you are upgrading or downgrading the boot loader image as well. When this is checked,
Boot Loader Image drop-down	This value is enabled when the **Select Boot Loader Image** checkbox is selected. The drop-down list provides the Oracle SDM Cloud's best effort matching with the selected software image.
Add	Upload a boot loader image to add to the repository.

1. Select the software image to upgrade your device(s) to.
2. (Optional) Click **Add** to upload a new software image to the repository.
3. (Optional) Select the **Select Boot Loader Image** checkbox to upgrade your boot loader image as well.
4. (Optional) Click **Add** to upload a new boot loader image to the repository.
5. Click **Next**.

The **Add NF Upgrade Work Order**, **Work Flow** page displays.

> **Note**
>
> The **Add NF Upgrade Work Order**, **Work Flow** link is disabled until you select a software image. If you have not selected a software image and click **Next** to go to the **Work Flow** page, the Oracle SDM Cloud displays the error, **Error: Please select a software image**.

Work Flow

The **Add NF Upgrade Work Order**, **Work Flow** page allows you to configure a work flow for your work order.

This page contains the following buttons and fields:

Reject New Call checkbox	Specify whether or not to reject new calls during the work order.
Active Call Threshold field	This value is enabled only when **Reject New Call** is selected. Specify the threshold of active calls so that the software upgrade process can decide when to reboot the device.
Health Score Threshold field	Specifies the health score threshold, in percentage, with which to use to determine if the devices are in a stable condition. **Note** This field is for HA pairs only.
Call shedding Timeout drop-down list	Specifies the time, in minutes, to allow for call shedding to reach the **Active Call Threshold** value. The minimum allowable value is 1 minute and the maximum is 60 minutes.
Restore Original Redundancy State After Upgrade checkbox	Select to restore original redundancy state after upgrade.

	Note This field is only for HA pairs only.
Pause and Unlock after Loading Software (and Boot) Image(s) checkbox	This affects **Push software image to the device** within the **Steps** dialog. When this field is selected, the **Push software image to the device** within the **Steps** dialog is automatically selected. When this field is un-selected, the **Push software image to the device** within the **Steps** dialog is automatically un-selected.
Delete Old Software Image checkbox	When selected, the Oracle SDM Cloud removes the old software and/or boot loader image from the device upon a commit.
Steps icon	When clicked, this button opens a dialog box containing a list of process flow steps to be carried out by the work order task. Beside each step is a pause checkbox. Select the pause checkbox for any step at which you want the Oracle SDM Cloud to pause during the work order process.

1. Enter values for the Work Flow parameters.
2. Click **Finish** to complete creating the work order.

The following lists the steps the Oracle SDM Cloud takes during an NF upgrade work order:

Step 0: Check available space at the device	If there is available space at the device, the work order proceeds to the next step.
Step 1: Verify the original software image exists on device	Checks that the original software image (the current image) exists on the device.
Step 2: Push software image to the device	Uploads new software image to the device.
Step 3: Do call shedding on original active device	Starts the call shedding.
Step 4: Edit image name in boot parameters	Sets the new image name in the device boot parameters.
Step 5: Reboot the device	Reboots the device.

Note

If any of the above steps fail, the work order fails.

The following lists the steps the Oracle SDM Cloud takes during an SBC HA pair upgrade work order:

Step 0: Check available space for both devices	If there is available space on both devices, the work order proceeds to the next step.
Step 1: Check status and health for both devices	Checks that the health scores on both devices are within bounds.
Step 2: Verify the original software image exists on both devices	Checks the original software image (the current image) exists on both devices.
Step 3: Push software image to both devices	Uploads new software image to both devices.
Step 4: Do call shedding on original active device	Starts the call shedding on the active device.
Step 5: Edit image name in boot parameters for the standby device	Sets the new image name in the standby device boot parameters.
Step 6: Reboot the standby device	Reboots the standby device.
Step 7: Check health of the standby device	Checks the healthscore of the standby device.
Step 8: Force switchover active becomes standby	Changes both devices' redundancy roles. • The standby device's redundancy role changes to 'Active'. • The active device's redundancy role changes to 'Standby'.
Step 9: Do call shedding on original standby device	Starts the call shedding on the original standby device.
Step 10: Edit image name in boot parameters for the new standby device	Sets the new image name in the new standby device's boot parameters.
Step 11 Reboot the new standby device	Reboots the new standby device.
Step 12: Check health of the new standby device	Checks the healthscore of the new standby device.

Note

If any of the above steps fail, the work order fails.

Add LRT Update Work Order

Adding a Local Route Table (LRT) Update work order prompts the **Add LRT Update Work Order Wizard** to begin.

Note

All target devices must have the `/code/lrt/` directory already created prior to the procedure or the work order fails.

There are 3 screens in the Wizard:

- **Devices**
- **Settings**
- **Route Sets**

> **Note**
>
> If the devices you select are SBCs running 8.x, and you associate route sets with 9.x parameters, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) displays an error message and does not create the work order.

To add a LRT work order:

1. Expand the **Work Order Manager** slider and select **Administration**.
2. Click **Add**.
   The **Select Work Order Type** dialog appears.
3. Select **LRT Update** and click **Apply**.
   The **Add LRT Update Work Order Wizard** launches, bringing you to the **Add LRT Update Work Order**, **Devices** page.

Devices

The Add LRT Upgrade Work Order, Devices page displays a table containing all device nodes being displayed in Device Manager that support Local Route Table (LRT). This page allows you to select the devices to be serviced by the work order. The table includes the following columns:

Name	The device node name. A device node can signify a standalone device or devices configured as a HA pair.
Version	The current running software image version on the node.
IP Address	The IP address of the device.
Platform	The platform of the device.
Product	The device product (for example, SBC).
Selected	Specifies if the device is targeted to be serviced via this work order.

The following buttons appear on this page:

Clear button	Removes all search criteria and de-selects all devices.
Search button	Create a search of NFs managed by the Oracle SDM Cloud based on specified criteria. You can filter based on the following: • **Name** • **IP Address**

	• **Version** • **Platform** • **Product** Click **Apply** to create the search or **Cancel** to exit out.
Clear Search button	Clears the table of the results of an existing search, but keeps the selected devices as-is.
Refresh icon	Refreshes the Devices table.
Expand All/Collapse All icon	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Expand All** icon is enabled.

1. Select the devices or HA pairs for which you want to create a work order by selecting the checkbox in the **Selected** column.
   Device selection for LRT uses the following rules:
   - Selecting a device group selects all devices and child devices
   - The selected devices can be of mixed device types, platform, and software version.
   - A maximum of 20 devices can be added to a work order.
2. Click **Next**.
   The **Add LRT Upgrade Work Order**, **Settings** page displays.

Settings

The **Add LRT Upgrade Work Order**, **Settings** page allows you to configure some logistical information about the work order.

1. Enter values for the following parameters:

Work Order Name field	Enter a unique name for this work order. This is a required field and you cannot select **Next** or move to **Route Sets** without entering a value here. The following naming conventions apply: • Names can contain only letters, numbers (0-9), or underscores (_). • Names cannot start or end with underscores. • Names cannot contain consecutive underscores. • Names cannot contain whitespaces.
Auto Commit checkbox	Specify whether you want to the work order to be automatically committed after it is successfully executed. By default this is

	disabled. When this feature is off, you must manually commit the work order.
Scheduled Start Time (UTC) checkbox	Specify whether you want to schedule a start time for this work order. When the checkbox is checked, the **Date** field and calendar become enabled. By default this is disabled.
Date/Time calendar	When **Scheduled Start Time (UTC)** is enabled, this calendar widget is enabled. Select the date and time you want to schedule this work order. This value is both displayed and stored in UTC.
Run Device Task concurrently checkbox	Specify whether you want to upgrade multiple devices concurrently. When this checkbox is selected, the **Behavior** and **Error Policy** parameters are disabled.
Behavior drop-down list	Specify the behavior when upgrading or downgrading multiple devices: • **Never pause** - The work order does not pause after each device is upgraded. This is the default value. • **Pause after every device** - The work order pauses after each device is upgraded. • **Pause only after first device** - Pause after upgrading or downgrading the first device only.
Error Policy drop-down list	Specify how to behave when an error is encountered during the work order: • **Log and proceed** - The device which failed upgrade is rolled back, but the work order continues on the remaining devices. • **Stop** - The device which failed upgrade is rolled back and the work order on the remaining devices is halted. • **Stop and rollback** - The work order stops and any devices that have already been upgraded are rolled back.
Operation Timeout (Min.) field	Specify how long (in minutes) the Oracle SDM Cloud waits before timing out on a work order. The default value is **15** minutes.

2. Click **Next**.
The **Add LRT Update Work Order**, **Route Sets** page displays.

Route Sets

The **Add LRT Upgrade Work Order**, **Route Sets** page provides a table listing all Route Sets stored in the repository and allows you to select the Route Set to use for this work order.

> **Note**
>
> If a route set is modified to include 9.x SBC parameters, you must remove any devices from the route set that do not support 9.x behavior.

The table displays the following information for each Route Set:

Name	The name for the new Route Set. This value must use alphanumeric characters only and cannot contain spaces.
# of Routes	The number of routes contained in the Route Set.
Device LRT File Name	The name used for this LRT file, which must match the LRT file name in the device configuration and its extension. The default file extension is .xml.gz.
Device LRT Configuration Name	The configuration name of the LRT associated with the route set. This value must match te configured name on the device.
Pub-Id Type	The Route Set's Pub-Id type.
Selected	When the checkbox is selected, the devices are targeted to be updated with the selected Route Set.

1. Select the Route Set for this work order.
2. Click **Finish**.

Use an Offline Configuration for a Device

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports provisioning network function (NF) devices by downloading offline configuration files, providing the user the option to select and define configuration parameters of one or many NF groups, generating a downloadable configuration file, called a Data Doc. After loading an offline configuration, you can make configuration changes and/or create binding variables. This allows the user the ability to create and manage NF configurations, without having to interact with each individual device.

To avoid having to manually export the configuration to each individual device, the Oracle SDM Cloud allows you to generate a spreadsheet that creates multiple device configuration files and maps all of the configuration variables to each of the devices.

Add Device Configuration Work Order

The Device configuration work order wizard allows you to select devices and select configurations to push to these selected devices, create work orders, edit existing work orders, and delete any unused work orders.

> **Note**
>
> From the Offline Configuration table, when you click the **Update** button, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) automatically opens the Device Configuration Work Order Wizard to ensure the work order is updated accordingly.

- **Devices**
- **Settings**
- **Offline Configurations**

To add a device configuration work order:

1. Expand the **Work Order Manager** slider and select **Administration**.
2. Click **Add**.
   The Select Work Order Type dialog appears.
3. Select **Device Configuration** and click **Apply**.
   The **Add Device Configuration Work Order Wizard** launches, bringing you to the **Add Device Configuration Work Order**, **Devices** page.

Devices

The Add Device Configuration Work Order, Devices page displays a table containing all device groups being displayed in Device Manager that have been added to the Configuration Manager. This table allows you to select the devices to be serviced by this work order. The table includes the following columns:

Name	The device group name. A device group can signify a standalone device or devices configured as a HA pair.
Version	The current running software image version on the group.
IP Address	The IP address of the device.
Platform	The platform of the device.
Product	The device product (for example, SBC).
Selected	Specifies if the device is targeted to be serviced via this work order.

The following buttons appear on this page:

Expand All/Collapse All icon	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Expand All** icon is enabled.
Clear button	Removes all search criteria and de-selects all devices.
Search button	Create a search of NFs managed by Oracle SDM Cloud based on specified criteria. You can filter based on the following: • Device Type • Name • IP Address • Version • Platform • Product
Clear Search button	Clears the table of the results of an existing search, but keeps the selected devices as-is.
Refresh icon	Refreshes the Devices table.
Expand All/Collapse All icon	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Collapse All** icon is enabled.

1. Select the devices or HA pairs for which you want to create a work order by selecting the checkbox in the **Selected** column.
   Device selection for Device Configuration uses the following rules:
   - Selecting a device group selects all devices and child devices.
   - If the selected offline configuration is for HA, you can only select HA devices. If the selected offline configuration is stand alone, you can only select stand alone devices.
2. Click **Next**.
   The **Add Device Configuration Work Order**, **Settings** page displays.

Settings

The Add Device Work Order, Settings page allows you to configure some logistical information about the work order.

1. Enter values for the following parameters:

Work Order Name field	Enter a unique name for this work order. This is a required field and you cannot select **Next** or move to **Offline Configurations** without entering a value here.

	The following naming conventions apply: • Names can contain only letters, numbers (0-9), or underscores (_). • Names cannot start or end with underscores. • Names cannot contain consecutive underscores. • Names cannot contain whitespaces.
Auto Commit checkbox	Specify whether you want to the work order to be automatically committed after it is successfully executed. By default this is disabled. When this feature is off, you must manually commit the work order.
Scheduled Start Time (UTC) checkbox	Specify whether you want to schedule a start time for this work order. When the checkbox is checked, the Date field and calendar become enabled. By default this is disabled.
Date/Time calendar	When **Scheduled Start Time (UTC)** is enabled, this calendar widget is enabled. Select the date and time you want to schedule this work order. This value is both displayed and stored in UTC.
Run Device Task concurrently checkbox	Specify whether you want to upgrade multiple devices concurrently. When this checkbox is selected, the **Behavior** and **Error Policy** parameters are disabled.
Behavior drop-down list	Specify the behavior when applying a work order to devices: • Never pause - The work order does not pause after each device is has completed. This is the default value. • Pause after every device - The work order pauses after each device has completed. • Pause ony after first device - Pause after the first device completes only.
Error Policy drop-down list	Specify how to behave when an error is encountered during the work order: • **Log and proceed** - The device which failed is rolled back, but the work order continues on the remaining devices. • **Stop** - The device which failed is rolled back and the work order on the remaining devices is halted.

	• **Stop and rollback** - The work order stops and any devices that have already completed are rolled back.
Operation Timeout (Min.) field	Specify how long (in minutes) the Oracle SDM Cloud waits before timing out on a work order. The default value is **15** minutes.

2. Click **Next**.
   The **Add Device Configuration Work Order**, **Offline Configurations** page displays.

Offline Configurations

The Add Device Configuration Work Orders, Offline Configurations page displays a table listing offline configurations relevant to the selected devices and allows you to select the offline configuration to use for this work order.

The table displays the following information for each offline configuration:

Name	The name of the offline configuration.
Software Version	The software version of the offline configuration.
Platform	The platform version of the offline configuration.
Description	A description of the offline configuration.

1. Select the offline configuration to use for this work order.
2. From the **Offline Configuration Spreadsheet** drop-down list, select the spreadsheet to use for this offline configuration.
3. Click **Finish**.
   Upon clicking Finish, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) validates the settings entered and produces an error if any settings are incorrect or missing.

Commit a Device Configuration Work Order

Once you have created a Device Configuration Work Order, you must commit the work order for the changes to take place.

1. On the **Work Order Manager** slider, select **Administration**.
2. In the **Work Order Administration** table, select the Device Configuration Work Order you are committing.
3. Click the **More Actions** icon and select **Commit**.
   The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides a confirmation dialog informing users that the changes cannot be reverted once they are committed.
4. Click **Yes** to continue to commit the work order. Click **No** to not commit the work order and return to the Work Order Administration table.

Rollback Device Configuration Work Order Changes

If you have created a Device Configuration Work Order that has not yet been committed, you can rollback the changes if needed. This sets all associated Network Functions (NFs) to their original state.

1. On the **Work Order Manager** slider, select **Administration**.
2. In the **Work Order Administration** table, select the Device Configuration Work Order you are changing.
3. Click the **More Actions** icon and select **Abort**.
   The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) reverts all associated NFs to their previous state.

8
Route Manager

The Route Manager allows the Network Function (NF) to determine next-hops and map E164, String, or Range to SIP URIs locally for routing determination and flexibility. By creating route sets, which can be used to generate XML Local Route Table (LRT) files, you can push LRT updates to devices using the Oracle® Session Delivery Management Cloud's (Oracle SDM Cloud)'s Work Orders functionality.

Route Sets

The **Route Manager**, **Route Sets** page displays a table containing a list of all Route Sets that have been created or updated by any user belonging to the user group of the logged in user. This page allows you to add and manage Route Sets.

The table displays the following columns:

Name	Name of the Route Set.
Lock State	Locked or Unlocked state of the Route Set. If a Route Set is locked, the user who locked that Route Set is displayed.
# of Routes	Number of routes within the Route Set.
Last Modified Time	Last modified timestamp.
Version	Version of the Route Set.
Devices Requiring Updates	The number of devices that need updating based on differences in version out of the total number of associated devices for a particular Route Set.
Device LRT File Name	Name of the Local Route Table (LRT) XML file.
Device LRT Configuration Name	Name of the LRT configuration.
Description	Description of the Route Set.
Notes	Notes for the Route Set.
Pub-Id Type	The Pub-Id-Type for each of the Route Sets. For example, String, E164, or Range.

The following buttons appear on this page:

+ Add button	Opens the Add Route Set page. For more information, see "Add a Route Set".
Search button	Opens the **Search** dialog box, allowing you to search the table based on specified criteria, as well as create and save filters.

Clear Search button	Clears the **Search** criteria.
Delete button	Deletes the selected Route Set from the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) database.
More Actions icon	Provides a drop-down list with the following additional actions for a selected Route Set: • **Retrieve LRT File** - Retrieves the LRT File from the device. • **Edit** - Opens the Edit Route Set page. For more information, see "Edit a Route Set". • **Copy** - Creates and opens a copy of the LRT File in the Copy Route Set screen with data already pre-populated. **Note** A copied route set has a fixed **Pub-Id Type** that cannot be changed. To change the pub-id type, you must select and copy a route set with that pub-id type. • **Lock/Unlock** - The Lock Button performs an operation lock for the selected Route Set, blocking other users from performing actions on the Route Set. Note that some actions are grayed out for a Route Set until you select the **More Actions** icon, **Lock**. The **Unlock** button displays when a Route Set is in the Locked state and is used to unlock the Route Set, making it available to other users with permissions. • **Manage Routes** - Opens the Manage Routes page for the selected device. For more information, see "Manage Routes". • **View LRT File** - Downloads the XML file in view only format. • **Update Device** - Redirects you to the Add LRT Update Work Order page.
Refresh icon	Refreshes the table entries by retrieving the list of Route Sets from the server based on the Search and paging criteria.

Add a Route Set

You can add a Route Set on the **Add Route Set** page.

1. On the **Route Manager** slider, select **Route Sets**.

The **Route Set** page displays.

2. Click the **+ Add** button.
   The **Add Route Set** page displays.
3. Complete the following fields:

Name field	Enter a unique name for the Route Set.
Device LRT Configuration Name field	Enter the device's Local Route Table (LRT) configuration name.
Device LRT File Name field	Enter the name of the device's LRT file name (ending in .xml.gz).
Pub-Id Type drop-down list	Select one of the following from the drop-down list: • **String** • **E164** • **Range**
Description field	Provide a brief description of the Route Set.
Notes field	Provide any other relevant notes regarding this Route Set.

4. Click **Apply** to save the Route Set and return to the Route Sets page, or click **Cancel** to discard your changes and return to the Route Sets page.

Edit a Route Set

To edit a route set, you must enable the lock operation for the selected Route Set to block other users from performing actions on the Route Set.

1. Expand the **Route Manager** slider and click **Route Sets**.
2. Select the Route Set you want to edit from the Route Sets table, click the **More Actions** icon, and select **Lock** to lock the Route Set.

> **Note**
>
> Until you lock the Route Set, the **Edit** action is grayed out and cannot be selected.

3. Click the **More Actions** icon and select **Edit**.
   The Edit Route Set page appears.
4. Update any values required and either click **Apply** to save the changes and return to the Route Sets page, or click **Cancel** to discard your changes and return to the Route Sets page.

Search for Route Sets

Users can search for a Route Set based on specific criteria and can choose whether to just conduct a search, or to save the search as a unique filter.

1. Expand the **Route Manager** slider and select **Route Sets**.

2. Click **Search** in the **Route Sets** pane.
   The **Search** pop-up box displays.
3. Complete any of the following fields on which to search:

Filter Name drop-down field	A drop-down with existing saved filter names in which you can also enter text to create new filters. This allows users the ability to either add new filters or select an existing filter to edit or delete. This field is empty by default. For more information, see "Add a Route Set Search Filter". **Note** Users can only see the filters which were created or last updated by users belonging to the same group.
Route Set Type radio button	Select the type of Route Set to search for.Valid values are: • **E164** • **String** • **Range**
Pub-Id field	(Displays when **Route Set Type** is set to **E.164** or **String**.) Enter the Pub-Id on which you want to search. This value supports either exact match or wildcard. Wildcard can be used as follows: • *NNNN • *NNNN* • NNNN* If **Route Set Type** is set to **E.164**, only numeric values (and the '+' sign) are accepted.
Route set Name drop-down list	Select one or more Route Sets from the drop-down list. When you click in this field, all available Route Sets display. Searches are then performed within the selected Route Set(s).
Range Start field	(Displays when **Route Set Type** is set to **Range** and **Range Value** is empty.) A numerical value in the format of E164 that specifies the start value for a contiguous range of DID telephone numbers.

	This value supports either exact match or wildcard. Wildcard can be used as follows: • *NNNN • *NNNN* • NNNN* Only numeric values (and the '+' sign) are accepted.
Range End field	(Displays when **Route Set Type** is set to **Range** and **Range Value** is empty.) A numerical value in the format of E164 that specifies the end value for a contiguous range of DID telephone numbers. This value supports either exact match or wildcard. Wildcard can be used as follows: • *NNNN • *NNNN* • NNNN* Only numeric values (and the '+' sign) are accepted.
Range Value field	(Displays when **Route Set Type** is set to **Range** and **Range Start** and/or **Range End** are empty.) This field supports exact match within Range (within Start and End range). This field does not support the use of wildcards.
Device Group browser button	Launches the **Select Device** dialog box. Select one or more devices and click **Apply** to continue or **Cancel** to exit. When you select a device within a device group, the device group is automatically selected. When multiple devices are selected, Route sets associated with all of those devices are displayed in the search results.
Device LRT File Name field	Searches for Route Sets associated with the provided LRT file name.
Device LRT Configuration Name field	Searches for Route Sets associated with the provided **LRT Configuration Name**.

When multiple criteria are specified, Oracle SDM Cloud returns a result only if all the criteria matches. If multiple devices and multiple Route Sets are selected, a result is returned if at least one criteria matches.

The **Search** pop-up box contains the following buttons and icons:

Save Filter button	Saves the current filter and the criteria you have set. Changing the filter name creates a new filter. Users can only create and save 10 filters. Once that threshold has been passed, the Oracle SDM Cloud displays an error message.
Search button	Once you have entered criteria, click **Search** to display search results.
Clear button	Clears all criteria.
Delete icon	Deletes the selected filter. Oracle SDM Cloud prompts you to confirm the delete or cancel.

Manage Route Set Search Filters

Users can add, edit, delete, and clear filters to search across Route Sets. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) only allows users to create a maximum of 10 filters per user.

Users are able to see only the filters created by or last updated by them or another member within the same user group.

Add a Route Set Search Filter

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Click **Search** in the **Route Sets** pane.
   The **Search** pop-up box displays.
3. **Filter Name**—Enter a unique name for this filter. The filter name must meet the following criteria:
   - Must be unique.
   - No less than 3 characters.
   - No more than 50 characters.
   - May only contain letters, numbers underscore, hyphen, or whitepace.
   - Cannot start with a number.
     Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) verifies the filter name.
4. Specify any criteria on which you want this filter to search. In addition to a value for **Route Set Type** selected, you must have at least one criteria specified to create a filter.
5. Click **Save Filter** to save this filter for future use or click the X to exit out and not save the filter.

Edit a Route Set Search Filter

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Click **Search** in the **Route Sets** pane.
   The **Search** pop-up box displays.
3. Select the filter you want to edit from the **File Name** drop-down list.

4. Update any criteria required and click **Save Filter** to save the changes and return to the Route Sets page or click the **X** to discard your changes and return to the **Route Sets** page.

Clear a Route Set Search Filter

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Click **Search** in the **Route Sets** pane.
   The **Search** pop-up box displays.
3. Select the **Filter Name** from the drop-down list and click **Clear**.
   The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) clears all criteria from the filter.

Delete a Route Set Search Filter

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Click **Search** in the **Route Sets** pane.
   The **Search** pop-up box displays.
3. Select the filter you want to delete and click the **Delete** icon.
   A Confirm dialog appears asking you to confirm you want to delete this filter.
4. Click **Yes** to proceed or **No** to cancel.

Override Locks

The **Override Log** functionality is a Route Manager feature designed specifically for administrator users.

This feature enables administrators to view and unlock route sets that are in a locked state, regardless of the user or user group that initially locked them. This feature allows administrators the ability to manage orphan route sets, particularly those created by users who have left the organization or moved out of their groups.

View and Search Locked Route Sets

The Override Lock screen displays all locked route sets across the system.

Administrators are able to view, search for, and unlock route sets.

1. Expand the **Route Manager** slider and click **Override Lock**.
   The Route Sets Override Lock page displays with the following columns:

Name	Name of the Route Set.
Lock State	Locked or Unlocked state of the Route Set. If a Route Set is locked, the user who locked that Route Set is displayed.
# of Routes	Number of routes within the Route Set.
Last Modified Time	Last modified timestamp.
Version	Version of the Route Set.
Notes	Optional notes for this Route Set.

Route Set Type	The type of Route Set; either **String**, **Range**, or **E164**.
Created By	The user who created this Route Set.
Updated By	The user who last updated this Route Set.
Action	The available action for this Route Set.

2. **Search**—Optionally enter a Route Set name to search.
3. **Clear Search**—Clears an existing search.

Unlock Route Sets

Administrators are the only users with permissions to override locked Route Sets.

To unlock a locked Route Set:

1. Expand the **Route Manager** slider and click **Override Lock**.
   The Route Sets Override Lock page displays.
2. Select the Route Set you want to unlock.
3. Click the **Unlock** button in the Action column.
   A confirmation box displays.
4. Click **Yes** to unlock the Route Set or **No** to cancel the action.

Manage Routes

The **Manage Routes** page contains the Manage Routes table containing all of the Routes for the selected Route Set. The Manage Routes table's columns differ based on the type of selected Route Set.

> **Note**
>
> To access the Manage Routes page for a Route Set, you must first place a lock on the Route Set by clicking the **More Actions** icon and selecting **Lock**.

By default, the following columns display for each route type:

The tables may include the following columns:

Range type	• **Range Start** - Start of the Pub-Id range. • **Range End** - End of the Pub-Id range. • **Session Establishment Data (SED)** - SED, or formula, for a route. • **Description** - Description of the route.
String and **E164** types	• **Pub-Id** - Pub-Id of the User in a route. • **Session Establishment Data (SED)** - SED, or formula, for a route.

	• **Description** - Description of the route.

The Manage Routes page contains the following buttons and icons:

+ Add button	Opens the Add Route page, allowing you to add a route to the Route Set. For more information, see "Add a Route To a Route Set".
Search button	Opens the Search dialog box to search for routes based on specified criteria.
Clear Search button	Clears the previously applied search criteria.
Find & Replace button	Opens the Find & Replace page, allowing you to search the route set for a particular value and replace it with a different specified value. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides users with the option to find and replace all matched results at once, or to find and replace results one by one.
More Actions icon	Provides a drop-down list with the following additional actions for a selected Route Set: • **Edit** - Opens the Edit Route page. For more information, see "Edit a Route". • **Copy** - Creates a copy of the route on the next-hop level. You must provide a different name for the new route. • **Import** - Launches the Import CSV File Wizard. For more information, see "Import a CSV File". • **Set Columns** - Opens the Set Columns dialog box, allowing you to select the table columns you want to see. The dialog also contains a **Reset** button that allows you to reset the columns back to their default values. • **Delete** - Deletes the selected route from the Oracle SDM Cloud database.
Refresh icon	Refreshes the table entries by retrieving the list of Routes for the Route Set from the back-end server based on the Search criteria.
Expand All/Collapse All icon	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Collapse All** icon is enabled.

Add a Route To a Route Set

To add a route to an existing Route Set:

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Select the Route Set to which you want to add a Route, click the **More Actions** icon, and select **Lock** to lock the Route Set.

> **Note**
>
> Until you lock the Route Set, the **Manage Routes** action is grayed out and cannot be selected.

3. Click the **More Actions** icon, and select **Manage Routes**.
   The Manage Routes page displays.
4. Click **+Add**.
   The **Add Route** page displays.
5. Complete the following required fields for a **Range** type of route:

Range Start increment	Start of the Pub-Id range.
Range End increment	End of the Pub-Id range.
Weighted checkbox	Select this checkbox if this route uses weighted routes. Until you check this checkbox, the **Weight** and **Priority** fields are grayed out. **Note** You can only add weighted next hops to weighted routes and non-weighted next hops to non-weighted routes.
Weight increment	Specify the weight, in increments of 10 and in the range of 0 - 65530, of this route. This field is disabled until **Weighted** has been selected.
Priority increment	Specify the priority of this route. This field is disabled until **Weighted** has been selected. Valid values are 0 - 65535.
Next Hop Type drop-down list	Specify the next hop type. Valid values are: • **Regex** • **Void**
Session Establishment Data (SED) field	Enter the SED, or formula, for the route.

Order field	Select the value used to order, by preference, route records or output of routes in the LRT that have the same Pub-Id to display from lowest to highest.
Preference field	Select the value used to order, by preference, route records or output of routes in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) that have the same Pub-Id to display from lowest to highest.
Destination Group ($DESTGROUP) field	Select the public identifier group that stores operational route set information.
Additional SED Properties menu	Click the arrow icon to expand the following SED properties: • **Next Hop (NEXTHOP)**—Select the numerical entry for the IP address, FQDN, session agent name, or session agent group name that can be used in the formula to generate the SED for a route record. • **Trunk Group ($TRUNKGROUP)**—Select the numerical entry for the alphanumeric string that can be used in the formula to generate the SED for a route record. • **Trunk Context ($TRUNKCONTEXT)**—Select the numerical entry for the alphanumeric string that can be used in the formula to generate the SED for a route record. • **Routing Number ($RN)**—Select the numerical entry for the telephone number or prefix that can be used in the formula to generate the SED for a route record. • **Carrier Identification Number ($CIC)**—Select the numerical entry for the numeric value used in the formula to generate the SED for a route record. • **User 1 ($User1) through User 5 ($USER5)**—Select the numerical entry for the alphanumeric value with a user-specific definable meaning that can be used in the formula to generate the SED for a route record. It can also be used for aggregating route records into groups. Once defined, use of this field must be consistent within the route set.

	• **SED Formula**—Select the numerical entry for the alphanumeric string that contains an expression used to define string concatenation and text replacement to generate the SED for a route record.

Complete the following fields for a **String** or **E164** type of route:

Pub-Id field	Enter the Pub-Id.
Additional Pub-Id Properties menu	Click the arrow icon to expand the following SED properties: • NPA ($NPA) • NXX ($NXX) • PUser1 ($PUSER1) • PUser2 ($PUSER2) • Pub-Id Formula
Weighted checkbox	Select this checkbox if this route uses weighted routes. Until you check this checkbox, the Weight and Priority fields are grayed out. **Note** You can only add weighted next hops to weighted routes and non-weighted next hops to non-weighted routes.
Weight increment	Specify the weight, in increments of 10 and in the range of 0 - 65530, of this route. This field is disabled until **Weighted** has been selected.
Priority increment	Specify the priority of this route. This field is disabled until **Weighted** has been selected. Valid values are 0 - 65535.
Next Hop Type drop-down list	Specify the next hop type. Valid values are: • **Regex** • **Void**
Session Establishment Data (SED) field	Enter the SED, or formula, for the route.
Order field	Select the value used to order, by preference, route records or output of routes

	in the LRT that have the same Pub-Id to display from lowest to highest.
Preference field	Select the value used to order, by preference, route records or output of routes in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) that have the same Pub-Id to display from lowest to highest.
Destination Group ($DESTGROUP) field	Select the public identifier group that stores operational route set information.
Additional SED Properties menu	Click the arrow icon to expand the following SED properties: • **Next Hop (NEXTHOP)**—Select the numerical entry for the IP address, FQDN, session agent name, or session agent group name that can be used in the formula to generate the SED for a route record. • **Trunk Group ($TRUNKGROUP)**—Select the numerical entry for the alphanumeric string that can be used in the formula to generate the SED for a route record. • **Trunk Context ($TRUNKCONTEXT)**—Select the numerical entry for the alphanumeric string that can be used in the formula to generate the SED for a route record. • **Routing Number ($RN)**—Select the numerical entry for the telephone number or prefix that can be used in the formula to generate the SED for a route record. • **Carrier Identification Number ($CIC)**—Select the numerical entry for the numeric value used in the formula to generate the SED for a route record. • **User 1 ($User1) through User 5 ($USER5)**—Select the numerical entry for the alphanumeric value with a user-specific definable meaning that can be used in the formula to generate the SED for a route record. It can also be used for aggregating route records into groups. Once defined, use of this field must be consistent within the route set. • **SED Formula**—Select the numerical entry for the alphanumeric string that

	contains an expression used to define string concatenation and text replacement to generate the SED for a route record.

6. Click **Apply** to save the route to the Route Set and return to the Manage Routes page or click **Cancel** to discard your changes and return to the Manage Routes page.

Edit a Route Within a Route Set

1. Expand the **Route Manager** slider and click **Route Sets**.
2. Select the Route Set to edit, click the **More Actions** icon, and select **Lock** to lock the Route Set.

> **Note**
>
> Until you lock the Route Set, the **Manage Routes** action is grayed out and cannot be selected.

3. Select the Route Set to edit, click the **More Actions** icon, and select **Manage Routes**. The Manage Routes page displays.
4. Select the route to edit and click **Lock** to lock the route.

> **Note**
>
> Until you lock the Route Set, the **Manage Routes** action is grayed out and cannot be selected.

5. Select the route to edit, click the **More Actions** icon, and select **Edit**. The Edit Route page displays.
6. Update any values required and either click **Apply** to save the changes and return to the Manage Routes page, or click **Cancel** to discard your changes and return to the Manage Routes page.

Search and Replace Routes

The Find & Replace functionality allows a user to search for a specific attribute value, and specify a replacement value for that attribute. Users can conduct a search and choose to either replace all values at once, or replace values one by one.

This functionality is performed with exact match values in both the **Find** input field and **Replace with** value and the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) performs the following validations on these values.

- **Range Start** and **Range End**—Allows numerical digits only or numerical digits starting with a +.
- **SED**—Cannot be empty in any type of route set.
- **Pub-Id**—Required for String and E.164 route set types. In the case of E.164, Pub-Id can only be numerical values or numerical values starting with a +.
- **Weight and Priority**—Valid ranges are **0-65530**.

Perform a Search and Replace

To perform a search and replace:

1. Expand the **Route Manager** slider and select **Route Sets**.
2. Select the Route Set to search, click the **More Actions** icon, and select **Manage Routes**. The Manage Routes page displays.
3. Click **Find & Replace**.
   The Find & Replace page displays.
4. Enter values and use the following buttons to perform a search and replace.

Select Attribute drop-down list	Select the attribute type on which you want to search. • Pub-Id • Session Establishment Data (SED) • Description • NPA • NXX • PUser1 • PUser2 • Pub-Id Formula • Next Hop Type • Order • Preference
Find field	Enter the value to be replaced.
Replace with field	Enter a new value to replace the old value. A valid value must be entered or the Oracle SDM Cloud displays an error. A confirmation dialog box displays asking the user to confirm the replacement. Click **Yes** to complete the action or **No** to cancel.
Find Next button	Finds the next matched value within the table and highlights the row. If no values match, a dialog appears stating "There are no matches found."
Replace button	Replaces the attribute value in the highlighted row.
Replace All button	Replaces all matched values for routes at once. A confirmation dialog box displays asking the user to confirm the action. Click **Yes** to complete the action or **No** to cancel.

	After performing this action, a summary screen appears providing the following details: • Targeted Routes/Next Hop • Successful replacements • Number of errors • Attribute name • Previous value of replaced routes attribute • replaced value of routes attribute • In the case of failure, a maximum of 5 failure reasons display.

The data in the Find & Replace screen is sorted based on **Pub-Id** or **Range Start** by default.

Import a CSV File

When a comma-separated values (CSV) file is imported, column definitions and minimum fields are required in the file. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) provides the Import CSV Wizard to guide the process of specifying the CSV file, file format, and mapping the CSV columns to the Oracle SDM Cloud's properties.

> **Note**
>
> If a Route Set is not present, you must create one. For more information, see "Add a Route Set".

To access the Import a CSV File Wizard:

1. Select **Route Manager**, **Route Sets**.
2. Select the Route Set for which you are importing a CSV file.
3. Lock the Route Set by selecting the **More Actions** icon and selecting **Lock**.
4. Click the **More Actions** icon and select **Manage Routes**.
   The Manage Routes page displays.
5. Click the **More Actions** icon and select **Import**.
   The Import CSV File Wizard displays.

There are 3 screens in the Wizard:

- File Selection
- CSV Column Assignments
- Confirmation

File Selection

The first page in the Import CSV wizard is **File Selection**, where you specify the CSV file.

1. Click **Browse** next to **LRT File to Import**, select the CSV file, and click **Open**.

2. Enter values for the following parameters:

File Delimiter drop-down list	Select from the following file delimiting method: • **Comma**
Template to Use drop-down list	Select an available template or leave this field blank. The drop-down lists only templates of the same type as the Route Set.

3. Click **Next**.
The **CSV Column Assignments** page displays.

CSV Column Assignments

The **CSV Column Assignments** page guides you through mapping the CSV columns to the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) properties.

If an existing template was not selected on the **File Selection** page, the **Route** drop-down fields are empty and you must assign column names.

> **Note**
>
> If you map the Session Establishment Data (SED) property to CSV file column, the two formula properties are disabled and the SED is used for the route and the formula.

1. Complete the following fields:

Operation drop-down list	Select from the following values: • **Add** - Select to add the route. • **Delete** - Select to delete the route.
Pub-Id drop-down list	Select the numerical entry for the alphanumeric string that contains an expression used to define string concatenation and text replacement to generate the Pub Id for a route record.
Additional PubId Properties menu	Click the arrow icon to expand the following Pub ID property entries that can be mapped to their corresponding CSV file column number: • **NPA ($NPA)**, **NXX ($NXX)**, **PUser1**, and **Puser2** fields - Select the route entry that has the alphanumeric value that has a user-specific definable meaning that can be used in the formula to generate the Pub-Id for a route record. It can also be used for aggregating route records into groups.

	Once defined, use of this field must be consistent within the route set.
Next Hop Type drop-down list	Select the type of next hop to be used in the formula to generate the SED.
Session Establishment Data (SED) drop-down list	Select the applicable SED.
Order drop-down list	Select the value used to order, by preference, route records or output of routes in the Local Route Table (LRT) that have the same pub-id to display from lowest to highest.
Preference drop-down list	Select the value used to order, by preference, route records or output of routes in Oracle Communications Route Manager that have the same pub-id to display from lowest to highest.
Destination Group ($DESTGROUP) drop-down list	Select the public identifier group that stores operational route set information.
Description ($DESCRIPTION) field	Add a description for the route. All routes created with the same pub-id reflect the last (newest) non-empty change made to the **Description** field.
Additional SED Properties menu	Click the arrow icon to expand the following SED property entries that can be mapped to their corresponding CSV file column number: • **Imported SED formula** - —Select the numerical entry for the alphanumeric string that contains an expression used to define string concatenation and text replacement to generate the SED for a route record. • **Next Hop ($NEXTHOP)** - Select the numerical entry for the IP address, FQDN, session agent name, or session agent group name that can be used in the formula to generate the SED for a route record. • **Trunk Group ($TRUNKGROUP)** - Select the numerical entry for the alphanumeric string that can be used in the formula to generate the SED for a route record. • **Trunk Context ($TRUNKCONTEXT)** - Select the numerical entry for the alphanumeric string that can be used in

	the formula to generate the SED for a route record. • **Routing Number ($RN)** - Select the numerical entry for the telephone number or prefix that can be used in the formula to generate the SED for a route record. • **Carrier Identification Code ($CIC)** - Select the numerical entry for the numeric value used in the formula to generate the SED for a route record. • **User 1** through **User 5** - —Select the numerical entry for the alphanumeric value with a user-specific definable meaning that can be used in the formula to generate the SED for a route record. It can also be used for aggregating route records into groups. Once defined, use of this field must be consistent within the route set.
Save As Template field	If the user does not select a **Template to Use** on the **File Selection** page, and has made a change to the CSV Column Assignments, they can save the mapping as a new Template File.

2. Click **Next**.

> **Note**
>
> The following fields are mandatory when importing a CSV file:
>
> - Operation
> - Pub-Id
> - Next-hop-type
> - SED
> - Range Start (when **Pub-Id** type is set to **Range**)
> - Range End (when **Pub-Id** type is set to **Range**)

The **Confirmation** page appears.

Confirmation

The **Confirmation** page displays the Import Sample table. This table displays the content of the first five rows of the imported CSV file.

1. If any errors appear in the **Failures** table, click **Back** to correct your route set mappings.

> **Note**
>
> If the number of errors exceeds a certain amount, the **Finish** button is disabled and you must fix these errors to enable the **Finish** button.

2. Click **Finish** if there are no errors or once errors have been corrected.

Manage Templates

The **Manage Templates** page displays a table containing the list of templates created by or updated by any user belonging to the same user group as the logged in user, that can be used when managing routes and importing CSV files.

The Manage Templates table contains the following columns:

Name	Name of the template.
SED Formula	Defined formula for the Session Establishment Data (SED).
Pub-Id Formula	Defined formula for the Pub-Id.
Pub-Id Type	The Pub-Id type for this Route Set. This can be one of the following: • E164 • Range • String

The following buttons appear on this page:

+Add button	Opens the Add Import Template page.
Delete button	Deletes the selected Import Template from the Oracle SDM Cloud database.
More Actions icon	Provides a drop-down list with the following additional actions for a selected Import Template: • **Edit** - Opens the Edit Import Template page.
Refresh icon	Refreshes the table entries by retrieving the list of Route Sets from the back-end server based on the Search and paging criteria.

Add Import Template

The **Add Import Template** page allows you to map CSV file columns to the Route properties in Route Management.

1. Expand the **Route Manager** slider and click **Manage Templates**.
   The Manage Template page displays.
2. Click **+Add**.

The Add Import Template page displays.

3. Complete the following fields:

Name field	The new import template name.
Pub-Id Type drop-down list	Select a row number to map it to the corresponding Pub-Id type in the CSV file from the drop-down list. The following Pub-Id types are supported: • E164 • String • Range
Operation field	Enter the corresponding CSV file field.
Pub-Id field	Enter the corresponding CSV file field.
Additional Pub-Id Properties menu	Enter the corresponding CSV file field.
Next Hop Type field	Enter the corresponding CSV file field.
Weighted checkbox	Select if the route set is weighted. When selected, the **Weight** and **Priority** fields are activated. **Note** You can only add weighted next hops to weighted routes and non-weighted next hops to non-weighted route sets.
Weight field	Enter the weight of this route set. This value must be a multiple of 10 and lie in the range of 0 - 65530.
Priority field	Enter the priority of this route set. Valid values are between 0 and 65535.
Session Establishment Data (SED) field	Enter the corresponding CSV file field.
Order drop-down list	Enter the corresponding CSV file field.
Preference drop-down list	Enter the corresponding CSV file field.
Destination Group ($DESTGROUP) drop-down list	Enter the corresponding CSV file field.
Description ($DESCRIPTION) field	Enter the corresponding CSV file field.
Additional SED Properties menu	Enter the corresponding CSV file fields.

4. Click **Apply** to save the template and return to the Manage Templates page or click **Cancel** to discard your changes and return to the Manage Templates page.

Edit Import Template

1. Expand the **Route Manager** slider and click **Manage Templates**.
2. Select the import template to edit, click the **More Actions** icon, and select **Edit**. The Edit Import Template page displays.
3. Update any values required and either click **Apply** to save the changes and return to the Manage Templates page or click **Cancel** to discard your changes and return to the Manage Routes page.

Device Association

The Device Association page displays the Device Association table, listing all of the Route Sets that have been associated with target devices. The Route Set represents the root of a collapsible row in the table with the rows of children being a list of associated Network Functions (NFs).

> **Note**
>
> - Users are able to see those route sets or devices to which they have access. Route sets are accessible when they are created by or updated by any user belonging to the same user group as the logged in user.
> - Route Manager is not supported for ECB devices.

The table displays the following columns:

Route Set/Device Group	The name of the Route Set and the NFs associated. Click the arrow to expand to show all associated NFs.
Software Version	The software version the Device Group is running.
Version on Device	The Route Set version being run on the devices.
Current Version	The latest Route Set version.
Needs Update	Whether or not the Route Sets need to be updated on the NF.

The following buttons appear on this page:

Retrieve LRT File button	Opens the **Retrieve LRT File** page. This button is only enabled when the user has selected a NF from the table.
Update Device button	Opens the **Work Order Wizard**, with **Work Order Type** set as **LRT Update**. The **Devices** and **Route Set** pages within the wizard are pre-populated with the mapping information from the LRT Inventory table.

	This button is only enabled when the user has selected a Route Set from the table.
Refresh icon	Refreshes the table entries by retrieving the list of Route Sets from the back-end server based on the Search and paging criteria.
Expand All/Collapse All icons	Expands and collapses all device nodes. When the devices are expanded, the **Collapse All** icon is enabled and when the devices are collapsed, the **Collapse All** icon is enabled.

Retrieve LRT File

By clicking the **Retrieve LRT File** button on the **Device Association** page, the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) creates a new Route Set by retrieving the LRT file from the selected Network Function (NF).

1. Expand the **Route Manager** slider and click **Device Association**.
2. Select the Device Group for which you are creating a new Route Set and click **Retrieve LRT File**.
   The **Retrieve LRT File** page displays.
3. Complete the following fields:

New Route Set Name field	Enter a name for the new Route Set.
Device LRT Configuration Name field	The configuration name of the Local Route Table (LRT) associated with the route set. This value must match the configured name on the device.
Device LRT File Name field	The name used for this LRT file, which must match the LRT file name in the device configuration and select its extension. The default file extension is .xml.gz.

4. Click **Apply** to save the new Route Set and return to the Device Association page or click **Cancel** to discard your changes and return to the Device Association page.

9

Administration

The Administration element allows you to manage email notifications by way of subscriptions and notification criteria on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

Manage Subscriptions

The **Subscriptions** page displays a table containing all subscriptions configured on the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).

The Subscriptions table displays the following columns for each subscription configured:

Selected	Clicking the checkbox selects or unselects the subscription.
Subscription Status	The status of this subscription.
Subscription ID	The email address associated with this subscription.

The Subscriptions page contains the following buttons and icons:

Add button	Launches the **Add Subscription** page, allowing you to create a new subscription. The Oracle SDM Cloud displays an error if the Subscription ID is not recognized.
Delete button	Deletes any Subscriptions with the **Selected** checkbox checked. A confirmation appears asking you to confirm the deletion.
Refresh icon	Refreshes the contents of the table.

Add a Subscription

1. On the **Administration** slider, select **Notifications**, **Subscriptions**.
   The **Subscriptions** page displays.
2. Click the **+Add** button.
   The **Add Subscriptions** page displays.
3. **Subscription ID**—Enter the Subscription ID of the recipient. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) validates that this ID adheres to the following rules:
   - Must be a unique value.
   - The email address is recognized.
   - No longer than 200 characters.
   - Number of recipients associated with the email address cannot exceed 50.

4. Click **Apply** to continue and create the subscription or **Cancel** to cancel out of the add operation.
   The newly created subscription displays in the **Subscription** table.

Delete a Subscription

1. On the **Administration** slider, select **Notifications**, **Subscriptions**.
   The **Subscriptions** page displays.
2. Select the **Selected** checkbox for the subscription you want to delete and click **Delete**.
   A confirmation dialog box displays asking you to confirm the deletion.
3. Click **Yes** to delete the subscription or **No** to cancel the delete operation and return to the Subscription page.

> **Note**
>
> You can delete up to 5 subscriptions at a time.

Set Notification Criteria

You must configure the criteria for which the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) sends email notifications.

These notification emails list the Severity of the trap in the Subject of email, and the following information within the email:

- Trap name
- Trap description
- Failed resource
- Trap source
- Name of device involved

The Notification Criteria page contains a table listing all Notification Criteria configured on Oracle SDM Cloud.

The Notification Criteria table contains the following columns:

Selected	Select an entry in the table by checking or unchecking the checkbox.
Name	Unique name of the Notification Criteria.

The Notification Criteria page also contains the following buttons and icons:

+ Add button	Launches the **Add Notification Criteria** page for you to create a new Notification Criteria.
Delete button	Deletes the selected Notification Criteria. When you click this button, a confirmation dialog displays asking you to confirm the deletion.

More Actions icon	• **Edit**: Launches the **Edit Notification Criteria** page for you to update existing Notification Criteria. • **View**: Displays the criteria for the selected Notification Criteria.
Search text box	Searches the table for the specified Notification Criteria.
Refresh icon	Refreshes the table contents.

Add Notification Criteria

1. Expand the **Administration** slider and select **Notifications**, **Notification Criteria**.
   The **Notification Criteria** page displays.
2. Click **+ Add**.
   The **Add Notification Criteria** page displays.
3. Enter the following information:

Name text box	Enter a descriptive name for this Notification Criteria. This value cannot be shorter than 3 characters or longer than 100 characters.
Trap Name drop-down list	Select the name of the trap for this Notification Criteria. **Note** When a value is selected for this field, the **Source IP** parameter is disabled, and if a value is specified for **Source IP**, this parameter is disabled.
Trap Severity drop-down list	Select the severity the trap must reach to initiate an email notification. **Note** When a value is selected for both this field and **Trap Name**, the **Source IP** parameter is disabled. If a value is specified for **Source IP**, and this field, **Trap Name** is disabled.

Source IP text box	Enter the Source IP address associated with this Notification Criteria. The Oracle SDM Cloud supports IPv4 only. **Note** When a value is entered for this field, the **Trap Name** parameter is disabled.
Block notification checkbox	Enables or disables a notification for the specified IP address.
Notify on clear trap checkbox	Enables or disables a notification when the following trap severity levels are cleared: • Emergency • Critical • Major • Minor **Note** This checkbox is only enabled when a value for **Severity** has been selected.
Enable Notification checkbox	When selected, email notifications are sent in case of a fault match.

4. Click **Apply** to create the Notification Criteria or **Cancel** to cancel the add operation and be returned to the Notification Criteria page.

Edit Notification Criteria

1. Expand the **Administration** slider and click **Notifications**, **Notification Criteria**.
2. Select the Notification Criteria to edit, click the **More Actions** icon, and select **Edit**. The **Edit Notification Criteria** page displays.
3. Update the Notification Criteria as necessary.

Note

The Name of the notification criteria cannot be edited.

4. Click **Apply** to accept the changes or **Cancel** to cancel the edit operation and return to the Notification Criteria page.
For more information on the Edit Notification Criteria fields, see "*Add Notification Criteria*".

View Notification Criteria

The view functionality allows you to view a read-only version of Notification Criteria details.

1. Expand the **Administration** slider and click **Notifications**, **Notification Criteria**.
2. Select the Notification Criteria to view, click the **More Actions** icon, and select **View**.
   A page displaying the following details for the selected Notification Criteria's displays.

Name	The unique name of the Notification Criteria.
Trap Name	The Trap Name associated with this Notification Criteria.
Severity	The severity of the Notification Criteria.
Source IP	The Source IP associated with this Notification Criteria.
Notify on clear trap	The status of the **Notify on clear trap** property.
Block Notification	The status of the **Block Notification** property. This works in conjunction with the **Source IP**, blocking notifications from that IP.
Enable Notification	The status of the **Enable Notification** property.

3. Click **OK** to exit out and return to the Notification Criteria page.

Delete Notification Criteria

1. Expand the **Administration** slider and click **Notifications**, **Notification Criteria**.
2. Select one or more Notification Criteria to delete and click **Delete**.
   A confirmation dialog box displays asking you to confirm the deletion.
3. Click **Yes** to delete the Notification Criteria or **No** to cancel the delete operation and return to the Notification Criteria page.

10

HDR Reports and Analytics

The HDR Reports and Analytics feature, in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud), provides a centralized platform for session delivery monitoring and management.

This feature enables reporting and analytics for Network Function (NF) data by integrating and processing Historical Data Records (HDR) groups from Session Border Controllers (SBC) and Enterprise Session Border Controllers (ESBC) devices. The raw data sent by these devices is processed, ingested, and aggregated into hourly, daily, weekly, and monthly granularities, making it readily available for generating reports. Users can leverage Oracle SDM Cloud Analytics to perform advanced visualization, analytics, and real-time monitoring of HDR data. Additionally, the feature supports historical trend analysis based on HDR statistics, allowing users to generate both pre-defined (canned) and custom reports.

> **Note**
>
> Reports and Analytics may take up to one hour to appear in Oracle SDM Cloud after being provisioned. Only users with the appropriate permissions are able to see the Reports and Analytics option in the dashboard slider menu. For more information, see *Application Roles*.

Users can perform the following functions with the HDR Reports and Analytics feature:

- Collect HDR data—Configure Collection Groups to enable the collection of Historical Data Records (HDR) from SBC/ESBC devices. A collection group consists of a set of parameters and devices designated for gathering HDR data, defining settings such as HDR groups, collection intervals, start and stop times, and push receiver details.
- Manage collection groups—Add new collection groups to include specific HDR data for monitoring and analysis. Edit existing collection groups to update configurations, such as descriptions, intervals, or HDR groups.
- Analyze HDR data—Leverage Oracle SDM Cloud Analytics for advanced visualization and analytics. Perform real-time monitoring of HDR data and historical trend analysis based on HDR statistics.
- Generate reports—Create custom reports tailored to specific metrics and analysis needs. Use canned reports for predefined analytics and insights.
- Monitor Network Function (NF) data—Access HDR statistics grouped by categories and types. Utilize record timestamps to analyze data within specific time windows.
- Integrate with SBC/ESBC Devices—Ensure SBC/ESBC devices are configured to forward HDR files in CSV format to Oracle SDM Cloud for processing and analysis.

Oracle SDM Cloud Analytics is session-based, meaning each user session lasts 24 hours from the time of the user's most recent login to Oracle SDM Cloud. Once this 24 hour window expires, Oracle SDM Cloud Analytics stops displaying data and users must log back in to Oracle SDM Cloud to establish a new 24 hour session.

> **Note**
>
> Oracle SDM Cloud Analytics ensures that users can only view data related to the devices they have been granted access to within Oracle SDM Cloud.

Application Roles

An application role in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics consists of a set of permissions that control what users can access and perform after logging in.

Your identity domain administrator is responsible for assigning the appropriate IDCS application roles to users or groups. Administrators can use the Oracle Cloud Infrastructure (OCI) Console to grant these roles to the relevant users or groups.

The OCI administrator can grant the following Oracle Analytics permissions to users and/or groups:

- ServiceUser—Allows users to create workbooks, connect to data sources, create datasets, load data for canned reports, create analyses, dashboards, and pixel-perfect reports, and share them with others.
- ServiceViewer—Allows users to view and run reports in Oracle Analytics (canned reports, workbooks, analyses, dashboards, pixel-perfect reports). This application role provides read-only access to Oracle Analytics.

> **Note**
>
> The following IDCS application roles in OCI are not used in Oracle Analytics:
>
> - ServiceAdministrator
> - ServiceDeployer
> - ServiceDeveloper

To assign application roles:

1. Log into the OCI console.
2. Navigate to **Identity**, **Domains**, **Default domain**, **Oracle Cloud Services**, **ANALYTICSINST_<instance-id>**.
3. Select **Application Roles**.
4. **Manage Users/Manage Groups**—Assign users and/or groups to the respective role.
5. Assign Users—Select the users and/or groups that you want and click **Assign**.

Pushing Data to the Oracle SDM Cloud

Devices push Historical Data Records (HDR) data to the Management Cloud Engine(s) (MCEs) in standard CSV format. The data is stored in the `/opt/oracle/mce/hdrData` directory on the MCEs, which act as the push receivers.

A push receiver is an SFTP destination server that receives the HDR records. The device establishes an SFTP connection to the push receiver(s) and transfers the CSV files.

Devices that are managed by multiple MCEs send HDR data to each associated MCE. The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) periodically monitors the push receiver directory, processing the HDR files used to generate reports and analytics.

If a Network Function (NF) is deleted from the Oracle SDM Cloud, users must stop the device's HDR sampling and pushing. To do this, access the device's CLI and execute the `request collection stop all` command.

Oracle SDM Cloud retains the removed NF's HDR data for 14 days. During this period, the NF can be re-added to Oracle SDM Cloud without losing HDR data. After 14 days, the NF's HDR data is purged.

File Types and Naming Conventions

Statistical records are forwarded from the device to the Management Cloud Engines (MCEs) for viewing in a comma-separated value (CSV) file.

Before a file is pushed by the device, the device creates a directory by group name for which the statistic belongs (for example, session-agent, system, etc.), if the directory does not already exist from a previous push.

Each file is named using the format `<UTC timestamp in seconds>.csv` (for example, 201112250000.csv).

Each CSV file contains the following:

- Header record—The first record of each file includes the statistical attribute name (for example, CPU Utilization, Memory Utilization, Health Score).
- Push interval and collection interval records—The file includes data records based on both the push interval and collection interval. For example, if the collection interval is one minute and the push interval is 15 minutes, the CSV file contains 15 records, one record collected every minute over the 15-minute push interval.

Time Granularity

The HDR Reports and Analytics feature in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) bases all time measurements on Coordinated Universal Time (UTC).

Devices sending data to Oracle SDM Cloud transmit raw data in UTC format. CSV data files are named using UTC timestamps in seconds, also known as Unix Epoch time.

Time Granularity for Data Aggregation and Reports

Aggregated data is available in the following time intervals:

- **Hourly**—Starts at the 00 minute of the hour and ends at minute 59.
- **Daily**—Starts at 00:00 (midnight) and ends at 23:59.
- **Weekly**—Starts at 00:00 on the first day of the week and ends at 23:59 on the last day.
- **Monthly**—Starts at 00:00 on the first day of the month and ends at 23:59 on the last day.

Canned reports are also available in Yearly intervals, which source data from monthly aggregated data.

> **Note**
>
> Aggregated data for each time granularity is dependent on its child granularity. For example, Hourly data is derived by aggregating the raw data, Daily data is derived by aggregating the hourly data, and so on.
> For example, to calculate the **Daily** Average CPU Utilization for a unique combination of device, redundancy state, and I2C bus state in the 'System' HDR group, the system aggregates the **Hourly** Average CPU Utilization records for that specific combination. Specifically, Oracle SDM Cloud computes the average of all **24 hourly records** (for the same unique combination) to derive the **Daily** value.
>
> This hierarchical aggregation ensures that data at each granularity level is consistent and accurately reflects the underlying metrics.

Data Visualization

The **Reports and Analytics**, **Data Visualization** option redirects users to Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics, where they can manage data visualizations and reports.

Upon selecting **Data Visualization** under the **Reports and Analytics** slider, a new browser window opens to the Oracle SDM Cloud Analytics page. If prompted to login, users can sign in using their existing Oracle SDM Cloud credentials.

> **Note**
>
> This feature is available only with on a commercial entitlement. For more information, see the Oracle SDM Cloud License Document.

For more information, see *Application Roles*.

Analytics Dashboard

The **Reports and Analytics**, **Analytics Dashboard** option redirects users to Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics, where they can view data visualizations and reports.

Upon selecting **Analytics Dashboard** under the **Reports and Analytics** slider, a new browser window opens to the Oracle SDM Cloud Analytics page. Ir prompted to login, users can sign in using their existing Oracle SDM Cloud credentials.

For more information, see *Application Roles*.

Collection Groups

Collection groups enable users to configure the collection, processing, and reporting of Historical Data Records (HDR) statistics from devices added to the collection group.

Collection groups streamline HDR data management, ensuring consistent monitoring and analysis across selected devices.

The following rules apply to collection groups:

- Collection groups can only be added to Session Border Controller (SBC) and Enterprise Session Border Controller (ESBC) devices if they are registered in both **Device Manager** and **Configuration Manager**.
- When creating a collection group, multiple devices or high-availability (HA) pairs can be selected. However, all selected devices must run the same software and platform version. If Management Cloud Engine (MCE) cross-site is configured, the devices must belong to the same MCE cross-site.
- Although multiple devices can be selected during creation, one collection group per device/HA pair is generated and configured upon applying the settings.
- A maximum of one collection group can be added to a standalone or HA pair device.

Collection Group Prerequisites

Before configuring a collection group, ensure SFTP is set up for pushing HDR data from Session Border Controller (SBC) and Enterprise Session Border Controller (ESBC) devices to the Management Cloud Engine (MCE) acting as the push receiver server.

To generate and export the host key:

1. Log in to the MCE server as the root user using the LAN/Private IP.

   ```
   su root
   ```

2. Navigate to the SSH directory.

   ```
   cd /etc/ssh
   ```

3. Generate the SSH host key using the following command.

   ```
   ssh-keygen -e -f /etc/ssh/ssh_host_rsa_key.pub
   ```

4. Copy the base64-encoded public key, ensuring it includes the BEGIN and END markers as specified by RFC 4716. For example:

   ```
   --- BEGIN SSH2 PUBLIC KEY ---
   <generated public key>
   --- END SSH2 PUBLIC KEY ---
   ```

5. Log into the SBC/ESBC device CLI and access admin mode.
6. Import the host key using the **ssh-key** command.

   ```
   ORACLE# ssh-key known-host import <mce_server_ip>
   ```

7. Paste the host key with the BEGIN and END markers at the cursor point.
8. Terminate the key input with a semicolon (;).
9. Save and activate the configuration.

   ```
   ORACLE# save-config
   ORACLE# activate-config
   ```

10. Verify the host key using the following command.

```
ORACLE# show running-config ssh-key
```

11. Repeat steps 5-10 for additional devices.

Add a Collection Group

You can add Collection Groups in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) to enable collecting Historical Data Records (HDR). This data is processed and made available for generating analytical reports based on metrics from Session Border Controllers (SBC) or Enterprise Session Border Controllers (ESBC) devices in the network.

- The user must have opted for the Reports and Analytics feature.
- The user's role must have appropriate permissions to access and configure this feature.
- The user must have completed prerequisite steps for configuring SFTP for HDR data push. See *Collection Group Prerequisites* for more information.
- Devices selected for the collection group must belong to the same software version, platform version, and Management Cloud Engine (MCE) cross-site model.

> **Note**
>
> For cross-site redundancy models, you must provide push receiver details for each MCE managing the selected devices.

1. Expand the **Reports and Analytics** slider and click **Collection Groups**.

   The **Collection Groups** page displays.

2. Click **Add**.

   The **Add Collection Group** page displays.

3. Enter the following **Group Configuration** parameters:

Name field	Enter a unique name adhering to the following: • Starts with either an alphanumeric value or an underscore (_) • Contains no special characters • Has a minimum length of three characters **Note** The device name is appended to the Collection Group name.
Description field	Add a brief description of the collection group.

Start Collection (UTC) calendar	Click the calendar to specify a start time for data collection or select **Now** to start immediately.
Stop Collection (UTC) calendar	Click the calendar to specify a stop time for data collection or select **Never** to enable continuous data collection. **Note** Oracle SDM Cloud displays an error message if a user attempts to input a **Stop Collection** time before the **Start Collection** time or if they try to set either of these times before the current time.

4. Select one or more devices from the list. Oracle SDM Cloud displays only the devices that support Reports and Analytics collection, meaning only SBC and ESBC devices configured in both Device Manager and Configuration Manager.

> **Note**
>
> When selecting multiple devices, the devices must be running the same version and platform. Therefore, upon selecting the first device, the tables updates to show only those devices running the same software and platform versions and on the same Management Cloud Engine (MCE) (if MCE cross-site is configured).

5. Click **Next**.

   If mandatory fields are not filled or if validation rules are violated, Oracle SDM Cloud displays an error message and does not allow a user to proceed.

6. Enter the following **Device Collections Params**:

Push Interval (1...120 minutes) field	The time (in minutes) for sending collected records to the push receiver(s). The minimum allowable value is 1 and the maximum is 120 minutes. The default value is 15 minutes. Oracle recommends this value to be greater than or equal to 5 minutes. **Note** This value must be greater than or equal to the **Global Collection interval (minutes)** parameter.

Global Collection interval (minutes) field	The time (in minutes) for a device to sample data records. The default value is 5 minutes. **Note** The **Push Interval** value must be greater than or equal to this parameter's value.

7. Select the HDR groups from which to collect data.
   - Use **Select All** to include all HDR groups or click the checkbox next to individual groups.
   - Edit the Collection Interval for each HDR group as needed. Each interval must be less than or equal to the **Global Collection Interval** and must have a minimum value of **1**.
8. Click **Next**.

   If mandatory fields are not filled or if validation rules are violated, Oracle SDM Cloud displays an error message and does not allow a user to proceed.
9. Enter the following **Push Receiver Info** parameters.

SFTP Server IP Address field	Enter the LAN IP (private IP) address of the MCE where data is to be sent. **Note** For cross-site redundancy models, provide push receiver details for each MCE managing the selected devices.
Username field	Enter the SFTP server username.
Password field	The SFTP server (MCE) password and the device's configuration passwords. Click **Edit** to enter and/or update the password.

   The Push Receiver Info page displays the SFTP Path for data storage and the Protocol, both in read-only formats.
   See *Pushing Data to the Oracle SDM Cloud* and *Collection Group Prerequisites* for more information.
10. Click **Finish** to complete the configuration.

Edit a Collection Group

Users with the appropriate permissions can edit existing collection groups. The Edit Collection Groups page enables users to update various settings, including descriptions, start and stop times, collection intervals, HDR groups, and push receiver details.

The edit functionality is accessible only when the collection group is in one of the following statuses:

- Configured
- FailedStart
- Stopped

> **Note**
>
> If a device associated with an active collection group is removed from the Configuration Manager, the collection group automatically stops and its status updates to 'Stopped'. An informational message displays, and the **Edit** and **Collection Group Action** buttons are disabled.

To edit a collection group:

1. Navigate to **Reports and Analytics**, **Collection Groups**.

   The **Collection Groups** page displays with a list of all available collection groups.
2. Select the collection group to edit by clicking the corresponding table row and click **Edit**.

   > **Note**
   >
   > The **Edit** button is disabled if the collection group is in any status other than **Configured**, **FailedStart**, or **Stopped**. If the collection group is active, click the **Stop Collection** button to halt the collection process and enable the **Edit** button.

   The **Edit Collection Group** page displays.
3. Edit the **Group Configuration parameters** that require updates and click **Next**.

   > **Note**
   >
   > The **Name** and device selection are read-only.
4. Edit the **Device Collections Params** parameters that require updates and click **Next**.
5. Edit the **Push Receiver Info** parameters that require updates and click **Finish**.

   > **Note**
   >
   > The **SFTP path for data storage** and **Protocol** fields are read-only.

6. Monitor the collection group status on the Collection Groups page. The status updates to **Configuring** during the process and changes to **Configured** upon successful completion. If the operation fails, the status displays as **FailedConfiguration**.

Delete a Collection Group

Users with appropriate permissions can delete collection groups.

The delete functionality is not accessible when the collection group is in one of the following statuses:

- Active
- FailedStop

To delete a collection group:

1. Navigate to **Reports and Analytics**, **Collection Groups**. The **Collection Group** page displays with a list of all available collection groups.
2. Select the collection group to delete by clicking the corresponding table row.
3. Click **Delete**.
   A Confirmation dialog appears asking you to confirm you want to delete that collection group.
4. Click **Yes** to proceed or **No** to cancel.

View a Collection Group and its Logs

Users with appropriate permissions can access collection groups, view collection groups, and view collection group logs.

To view collection groups:

1. Expand the **Reports and Analytics** slider and click **Collection Groups**.
2. Select the collection group you want to view, click the **More Options** icon, and select **View**.
   The collection group configuration displays without interrupting the collection process.

To view collection group logs:

1. Expand the **Reports and Analytics** slider and click **Collection Groups**.
2. Select the collection group whose logs you want to view, click the **More Options** icon, and select **Logs**.
   The **Collection Group Logs** pop-up window displays with various information related to the collection group's configurations and activities.
3. Optionally, users can click **Save to File** to download a copy of the Logs locally.

Set a Retention Policy

After data collection starts, Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) consolidates the raw data into various time-based categories, such as hourly, daily, weekly, and monthly. This task allows you to adjust the standard data retention period, which is initially set to 90 days for both raw and aggregated data. Any data that surpasses the retention limits you set will be automatically deleted on a nightly basis.

> **Note**
>
> Increasing retention times increases ADW usage. Ensure that the ADW has enough storage to store the data according to the configured retention period.

To set a retention policy:

1. Navigate to **Reports and Analytics**, **Retention Policy**. The **Retention Policy** page displays.
2. Select a **Retention Period** from the drop-down list and click **Apply**.

> **Note**
>
> When opting for Reporting and Analytics, discuss your retention requirements with your Oracle representative as the default retention period is 90 days and users must update this value manually.

Canned and Custom Reports

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) supports two types of reports, canned reports and custom reports.

Canned reports provide users with pre-configured, out-of-the-box reports and visualizations to analyze network trends and monitor key performance indicators (KPIs). They are designed to offer a head start for users in understanding their network data without requiring custom report creation.

Available canned reports:

- Performance—Displays CPU, memory, registration cache, and concurrent sessions.
- Physical Interface—Displays octets, packets on interface, error, and discard trends.
- QoS—Displays RFactor, major exceeded, critical exceeded, and successful sessions.
- SA-SRTP—Displays Total Secure Real-Time Protocol (SRTP) SA Add, Modify, and Delete request statistics.
- Security—Displays requests and message status, ACL entry promotions, and demotions.
- Session Realm—Displays calls per second, QoS RFactor, answer seizure ratio, and one-way signaling latency.
- SIP Policy—Displays total local policy lookup statistics and the total number of requests challenged.
- Summary—Displays sessions, session state, dialogs, and errors.

If the canned reports do not meet their needs, users can create custom reports and visualizations in the Oracle SDM Cloud Analytics environment. This flexibility empowers users to tailor their data exploration and presentation to specific requirements.

Custom reports can be created in two ways: by duplicating and modifying an existing canned report or by building a new report from scratch.

> **Note**
>
> To view and interact with canned reports in Oracle SDM Cloud Analytics, users must have either the ServiceUser or ServiceView application role to access the Shared Folders directory.

Run a Canned Report

Canned Reports are predefined reports that run on both raw and aggregated Historical Data Records (HDR). These reports provide insights into various network monitoring KPIs.

To run a canned report:

1. Navigate to **Reports and Analytics**, **Data Visualization**.
   Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics opens in a new tab.
2. If prompted, sign in using the same account credentials as Oracle SDM Cloud.
3. Expand the Navigator icon, click **Catalog**, and navigate to **Shared Folders**, **Canned Reports**.
4. Select one of the following folders:
   - Performance
   - Physical Interface
   - QoS
   - SA-SRTP
   - Security
   - Session Realm
   - SIP Policy
   - Summary
5. Double-click the report you want to open.
   The Oracle SDM Cloud Analytics fetches and plots the latest data.

   Users can do the following:
   - Explore various Dashboards and Canvases within the workbook.
   - Apply filters for granular data analysis

   > **Note**
   >
   > Users are not permitted to edit and save reports directly within the Canned Reports directory. To modify canned reports, users must first create a duplicate of the report and then make their edits to the duplicated version.

   The following screenshot shows two examples of canned reports.

Create a Custom Report From a Canned Report

As editing and saving reports directly in the Canned Reports directory is not allowed, users can duplicate canned reports as one way to create their own custom reports.

To duplicate a canned report to edit and save:

1. Navigate to **Reports and Analytics**, **Data Visualization**.
   Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics opens in a new tab.
2. Sign in using the same account credentials as Oracle SDM Cloud.
3. Click the **Options** icon and select **Open Classic**.
4. Click **Catalog**.
5. Select **Shared Folders**, **Canned Reports** and click the **Copy** icon.
6. Navigate to the **My Folders** directory and click the **Past** icon.
   A new custom copy of the Canned Reports directory, containing all of the canned reports is created.
7. Edit the report and save your changes.

Create a Dataset From a Subject Area

The Custom Report Creation feature in Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics enables users to design tailored reports and visualizations based on Historical Data Records (HDR) data.

This feature leverages Oracle SDM Cloud Analytics to provide flexible and advanced data analysis capabilities. Users can create visualizations directly from default subject areas or custom datasets, allowing for precise control over the data presented in reports.

Oracle SDM Cloud Analytics provides a default Subject Area called **OSDMC_ANALYTICS_SUBJECT_AREA**, which can be used to create visuals directly.

Users can create their own datasets based on specific subject areas and then utilize these customized datasets to produce visual representations.

> **Note**
>
> Only users belonging to the **ServiceUser** IDCS application role have permission to create new datasets.

There are two ways in which users can create a dataset from the Subject area:

- Users can create a dataset by selecting existing tables from the Subject area.
- Users can create a dataset by creating a custom table with selected columns.

Create a Dataset Using Existing Tables

Users can create a dataset by selecting existing tables from the Subject area.

1. Navigate to **Reports and Analytics**, **Data Visualization**.

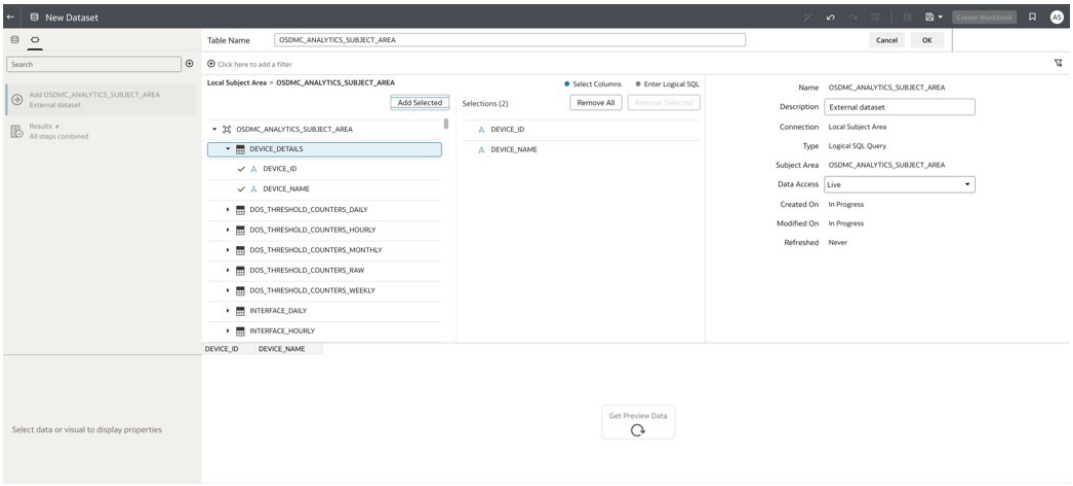
   Oracle SDM Cloud Analytics opens in a new tab.
2. If prompted, sign in using the same account credentials as Oracle SDM Cloud.
3. Click **Create** and select **Dataset**.

> **Note**
>
> If the **Create** button is not visible, the user does not have the appropriate permissions.

4. Select **Local Subject Area**.

5. From the left navigation pane, drag and drop the OSDMC_ANALYTICS_SUBJECT_AREA onto the **Join Diagram** canvas.
6. Select **Edit Definition**.

7. Select the tables you want to add and click **Add Selected**.



> **Note**
>
> To ensure proper data association, Oracle recommends adding the DEVICE_DETAILS table (which includes the DEVICE_NAME column) to all relevant datasets and tables.
> To join the DEVICE_DETAILS table with associated tables, click and hold the **Circle** icon on the DEVICE_DETAILS table, then drag and drop it onto the desired tables.

8. Select the **Data Access** type from the drop-down to specify the caching options for data in this Dataset.
9. Optionally, preview the data present by clicking **Get Preview Data**.
10. Enter a **Table Name** and click **OK**.
11. Repeat steps 5-10 to add all required tables.
12. Click **Save** and enter a Dataset Name when prompted.

    This dataset is now available and can be used to create visualizations in within workbooks.

Create a Dataset Using a Custom Table

If you do not select an existing table from the Subject area, you can create a custom table by selecting specific columns.

1. Navigate to **Reports and Analytics**, **Data Visualization**.

Oracle SDM Cloud Analytics opens in a new tab.

2. If prompted, sign in using the same account credentials as Oracle SDM Cloud.

> **Note**
>
> Only users belonging to the **ServiceUser** IDCS application role have permission to create new datasets.

3. Click **Create** and select **Dataset**.

> **Note**
>
> If the **Create** button is not visible, the user does not have the appropriate permissions.

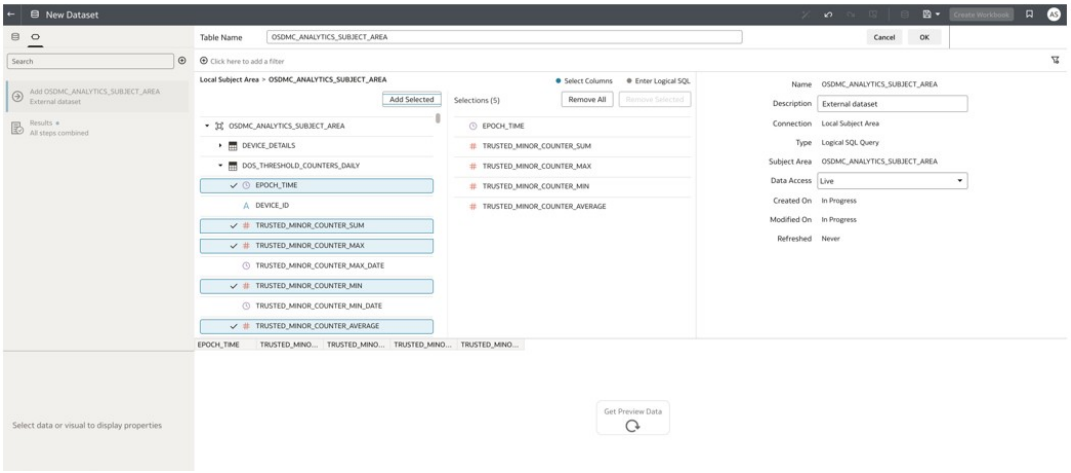
4. Select **Local Subject Area**.

5. From the left navigation pane, drag and drop the OSDMC_ANALYTICS_SUBJECT_AREA onto the **Join Diagram** canvas.
6. Select **Edit Definition**.

7. Select the columns to add from the existing tables and click **Add Selected**.

   For example, in the below example, the user has the following columns selected:

   - TRUSTED_MINOR_COUNTER_SUM
   - TRUSTED_MINOR_COUNTER_MAX
   - TRUSTED_MINOR_COUNTER_MIN
   - TRUSTED_MINOR_COUNTER_AVERAGE
   - DEVICE_NAME



> **Note**
>
> - Do not add columns from multiple source tables into a single dataset table, as this may result in misleading or invalid visualizations and data.
> - To ensure device specific data while generating visualizations, Oracle recommends adding the DEVICE_NAME column to all tables.

8. Select the **Data Access** type from the drop-down to specify the caching options for data in this Dataset.
9. Optionally, preview the data present by clicking **Get Preview Data**.
10. Enter a **Table Name** and click **OK**.
11. Repeat steps 5-10 to add all required tables.
12. Click **Save** and enter a Dataset Name when prompted.

    This dataset is now available and can be used to create visualizations in within workbooks.

Create a Custom Workbook

Users can create custom workbooks, or reports, either from the dataset or the subject area.

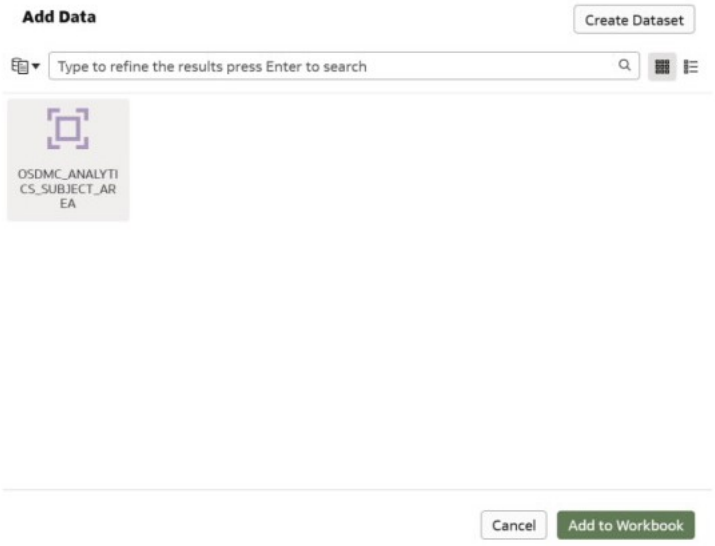
For more information on working with workbooks, see Begin to Build a Workbook.

> **Note**
>
> Only users belonging to the **ServiceUser** IDCS application role have permission to create new reports and visualizations.

To create a custom workbook:

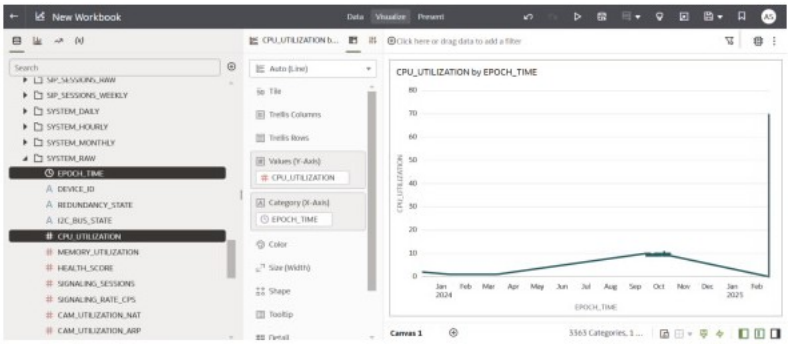
1. Navigate to **Reports and Analytics**, **Data Visualization**.
   Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Analytics opens in a new tab.
2. If prompted, sign in using the same account credentials as Oracle SDM Cloud.
3. Click **Create** and select **Workbook**.

4. Select the dataset from which you want to create the workbook. Use either the default subject area, OSDMC_ANALYTICS_SUBJECT_AREA or select a custom dataset.



   For more information on creating visualizations, see *Create a Dataset from a Subject Area*.

5. Click **Add to Workbook**.
6. Under **Data** in the left navigation, select the dataset, select the tables, and select the columns you want to visualize.
7. Drag and drop the selected columns onto the canvas.



   Oracle SDM Cloud Analytics creates and displays a visualization based on the selected columns.

8. Optionally, modify the visualization by configuring various properties of the visualization.
9. Optionally use filters to focus the data in your workbooks. For more information, see About Visualization Properties and Adjust Visualization Properties.
10. Click the **Save** icon and save the worbook in a sub-folder under either My Folders directory or Shared Folders directory.
    Once saved, the workbooks are available to be exported and shared in various formats. See Import, Export, and Share for more information. Oracle SDM Cloud Analytics supports various analytical capabilities such as Outlier detection and Clustering.

> **Note**
>
> Workbooks saved under My Folders are local to the user and cannot be overwritten during upgrade. Workbooks saved under Shared Folders are accessible to all users, but are vulnerable to be overwritten during upgrade.