Oracle® Communications Session Delivery Manager
Administration Guide

Release 8.0

June 2018

ORACLE®

Oracle Communications Session Delivery Manager Administration Guide, Release 8.0

Contents

ORACLE

4   Security Manager

5   Fault Manager

6   Manage Transport Layer Security Certificates

7   Configure Northbound Interface Traps

8   Monitor Session Delivery Manager Server Health and Disk Usage

9   Session Delivery Manager Server Database Maintenance

10   Session Delivery Manager Server Cluster Maintenance

A   Available Session Delivery Manager Server Scripts

B   Fault Trap Notification Contents

List of Figures

List of Tables

About This Guide

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

> **✎ Note:**
>
> With the introduction of the product plugin service and changes in the SDM product, only the Oracle Communications Session Delivery Manager Documentation Library appears in this section of each SDM guide.

Related Documentation

Table 1   Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • Implement SDM on your network as a standalone server or high availability (HA) server. • Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	Provides the following installation information: • Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons. • Do the typical installation to perform the minimal configuration required to run the SDM server. • Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.

ORACLE®

Table 1   (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the SDM feature support new to this release.
Security Guide	Provides the following security guidelines: • Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. • Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

Revision History

Date	Description
August 2017	Initial release
November 2017	Information was added about Mult-NIC environments in the *Caveats and Limitations* section.
May 2018	A note was added to the *Manage Transport Layer Security Certificates* chapter that states that this chapter does not address the importation or deletion of HTTPS Certificates for the web service.
June 2018	The *Use Server Diagnostics* section was added to the *Session Delivery Manager Application Overview* chapter.

1
Implement Session Delivery Manager on Your Network

Use the information in this chapter to help you implement Oracle Communications Session Delivery Manager on a standalone server or high availability (HA) server cluster on your network before you install and configure SDM.

Session Delivery Manager Server Components

The following SDM server components are supported on standalone and clustered systems to ensure that SDM application services run without failure.

- **Load balancer**—This service provides SSL security (HTTPS) and load balances traffic among all front-end cluster nodes to ensure that there is no single point of failure. Access to SDM services is not denied if at least one node is running.

- **Front-end server**—This node maintains client interaction support by managing sessions and performing authentication and authorization functions, and targets a local back-end server by default.

- **Back-end server**—This node runs the services required to support any functionality provided by SDM. For example, the back-end server can provide route management, fault management, or configuration management functionality. The back-end server also hosts the embedded database and the message services, which are responsible for maintaining the distributed data flow and provides redundant failover capabilities.

- **Embedded database service**—The Berkley XML in-memory database supports the cluster by providing database replication services by negotiating the allocation of the master database among all nodes. The database service (DBS) provides the database functionality in the back-end server. On any host, one database instance is a local database and the other database instance is part of a replication group.

- **Message service**—The Message Oriented Middleware (MOM) service is used in the back-end server to support distributed message queues and topics. MOM is supported by the distributed event and data service (DEDS), which allows components to publish and subscribe to message topics and queues.

Cluster Data Distribution Techniques

An SDM cluster groups server nodes to offer reliable access to SDM system application services without disruption when failure condition(s) occur. The cluster support ensures that all submitted tasks can be processed as long as one member node is available.

The following data distribution techniques are used on an SDM server cluster to configure devices, deliver messaging information, protect and maintain the cluster database, and transfer files within the cluster:

- **Device configuration**—Any cluster node can go to a device on-demand to retrieve its most recent configuration. This allows each node to be synchronized to have the same configuration version, which prevents the need to replicate large datasets between nodes.

- **Message driven data**—Some data sets that can be subject to network latency such as fault management events, polling statistics and audit trails are distributed through a Message-Oriented Middleware (MOM) service, which provides asynchronous processing to an SDM system, so that this system can scale resources both vertically and horizontally. The resilience of the MOM is maintained by guaranteed deliveries and durable subscribers. The data is generally stored on the local host machine in a dedicated local database.

- **Database replication**—Sensitive data sets such as local configuration view (LCV), user security, and device management are transactional and need to be available over the cluster are maintained by a database replication group, which maintains one master database in the cluster at all times while all other members are replicas. Retrieval of datasets is done on the local host machines. However, transactional modifications to the data are done on the master database, which then replicates the transaction to the replicas. Replication keeps the cluster database synchronized. If the master database fails, the remaining replicas elect a new master database.

- **Push-pull file transfer**—Large datasets such as route sets, which are maintained in the local database or file system, are transferred around the cluster through push and pull mechanisms. Host nodes use the MOM service to publish that datasets are available through events, while other nodes use SFTP to pull information from other nodes or push information to other nodes.

Database Group Replication Data Content

Database group replication data cannot be compromised and is guaranteed to be replicated throughout the cluster to ensure that failover is not disruptive. Replication data includes:

- User management data, user credentials for authentication, and user access control lists (ACL) for authorization are included.

- The Local Configuration View (LCV) is a small dataset that contains the modifications users make to a targeted device configuration only to reduce the latency introduced when replicating larger datasets.

- Distributed locking data contains information for when an SDM lock has been placed on a targeted device for a specific operation to ensure that no two operations can occur concurrently on the same device.

- NF device group details are created when a device is added to SDM for management. This dataset provides the information required for SDM to communicate with the targeted product plugin and provide relevant hardware, firmware, configuration and reachability status.

- The SDM configuration dataset contains required user-customized configuration information for SDM services. For example, when the following types of changes are made in the configuration service, they are replicated to all hosts in the SDM cluster:

  - User

  - Global parameter variables

  - Reusable configuration module (RCM)

  - Offline configuration

- The fault sequence number, which is a global unique ID, is required to give distributed items uniqueness.

- Product plugin data is replicated, which includes its status and version information.

Select a Cluster Strategy

You can select a high-availability (HA) strategy that uses either a multi-node cluster or a two-node cluster.

A two-node cluster has a single master with one replica database, as shown below:
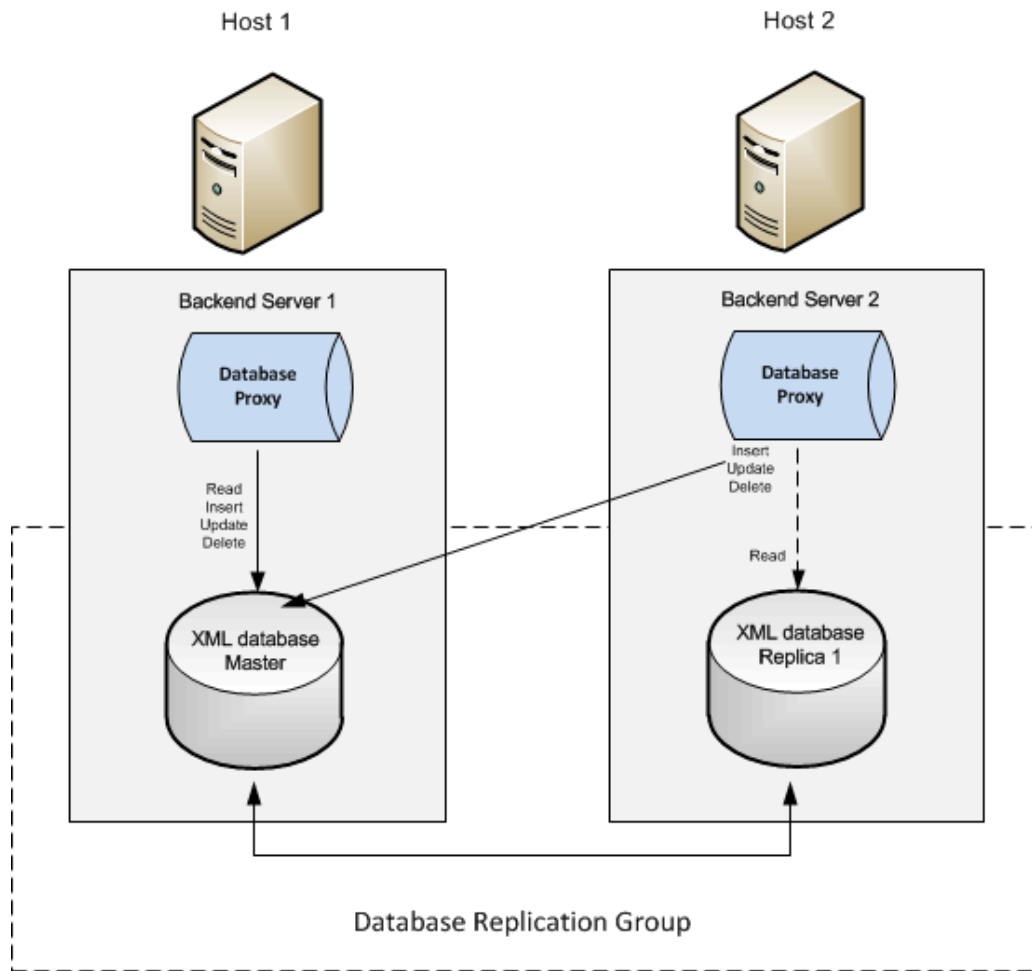
A three-node cluster has a single master with two replica databases for a higher level of HA:
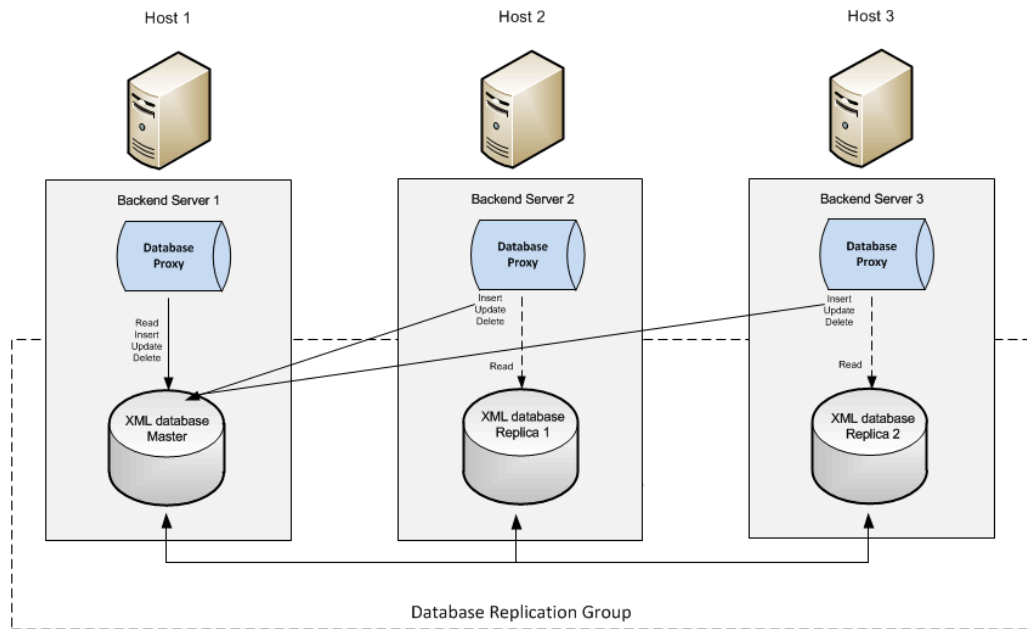
The following information describes the characteristics of a two-node or multi-node cluster:

* Each host is running a backend server with an embedded-in-memory Berkeley XML database.

* In the replicated group, there is only one master database and one or more replicas.

* The master database is responsible for distribution of transactional modifications to other replicas in the cluster.

* All back end server components interact with the database through a database proxy.

* The database proxy determines if the request for service is a transactional modification or a request for data retrieval. All data retrievals are done on the local database irrespective if it is a replica or master database. Requests for transactional modifications (inserts, updates or deletes) are forwarded from the database proxy to the master database in the cluster.

* The master database guarantees the transactions on a quorum basis in a cluster. This means that in a two-node cluster, one node must be up, in a three-node cluster two nodes must be up and so on. The majority of active members need to reply that they have received the replicated datasets before the master returns success on the transaction.

* User transactional latency is accounted for by detection of the late arrival of replicated data. Best effort replication is provided, which can mean the call might return before the dataset appears on the replicated databases. The database transactional layer offers additional support with latency in replicated data.
For example, a user on Host 3 starts a local transaction with the database proxy to insert content into the database. The database proxy in turn starts a transaction with the master database on Host 1. Each transaction that is started with the master database has a transactional ID associated with it. The master database uses best effort in ensuring that the datasets are replicated to the other members of its replication group.

However, if the best effort time is exceeded and the master database has received replies from quorum (the other replicas); the master database returns success. Returning success guarantees replication will occur at some point. The database Proxy on host 3 waits until the required transactional ID appears in its local replicated database before returning success on the transaction to the user on Host 3. This guarantees that the content inserted

on the Master database has reached the replicated database. Users that initiate transactions are guaranteed to see the outcome of those transactions in their local database independent of which host the original transaction was initiated.

Two Node Cluster Database Operations

Operation	Description
Server startup	When an Oracle Communications Session Delivery Manager server is started it joins the cluster as a replica and election is held if there is currently no master. If the member ends up as a replica, then it is synchronized with the master during the initialization phase of the database service startup. With the introduction of Oracle Communications Session Delivery Manager, Release 8.0, use the following steps to start an SDM server cluster: 1. Select one server to start in the cluster only. 2. Once the server you selected is started and operational, you can start the other server in the two-node cluster.
Master member failure	When the master fails the remaining replica becomes the new master.
Transactions (Quorum)	Transactions return successfully if a majority of the members in the cluster have replied that they received the replicated datasets. If quorum in replies from replicas is not achieved in a specific time period, the transaction fails.
Network partition	When the master fails the remaining replica becomes the new master.
Elections	An election can be won with a single vote. This allows the replica to be elected master in the case the master fails.
Recovery after a network partition	In a two node cluster it is possible for the network connection between the master and replica to be partitioned or become unresponsive due to network latency. In this situation an election is held and both nodes are elected and act as masters. While in this state, write transactions can occur at both sites. As a result, special handling is required after the partition is resolved and the system recovers from a two master configuration to a single master configuration: • Before the partition is resolved both nodes are in the role of master. • After the partition is resolved an election is automatically held to elect a master. • When the election is complete the node that wins remains the master and the other will become the replica. • The node that loses the election and becomes the replica tries to recover itself by restarting automatically if required if it had any write transactions that need to be rolled back to synchronize its database with the new master. Also, if the partition exists for more than 24 hours, Oracle recommends that you to take the cold backup from newly elected master and us it to restore the replica to avoid any data discrepancies.
Rejoining a cluster after graceful shutdown	An election can be won with a single vote. This allows the replica to be elected master in the case the master fails.
Rejoining cluster after shutdown for extended period	Perform a hot backup on the host running the master database before restarting a server that has been down for a long time. This avoids the potentially high cost synchronizing the server with the master during startup.

Multiple Node Cluster Database Operations

Activity	Description
Server startup	When an Oracle Communications Session Delivery Manager server is started it joins the cluster as a replica and an election is held if there is currently no master. If the member ends up as a replica, then it is synchronized with the master during the initialization phase of the database service startup. With the introduction of Oracle Communications Session Delivery Manager, Release 8.0, use the following steps to start an SDM server cluster: 1. Select one server to start in the cluster only. 2. Once the server you selected is started and operational, you can start the other server(s) in the cluster.
Master member failure	When the master fails or becomes partitioned from the rest of the members in the cluster, an election is automatically held by the remaining replicas to elect a new master.
Transactions (Quorum)	Transactions return successfully if a majority of the members in the cluster have replied that they received the replicated datasets. If quorum in replies from replicas is not achieved in a specific time period, the transaction fails.
Network partition	When a network partition exists between the members, only the members that can communicate with a majority of the members may elect a new master database. Members that can not communicate with a majority will enter READ-ONLY mode. Upon re-establishing network connectivity, re-elections take place and a master is elected while the other members revert to replicas.
Elections	In a cluster of three or more members, an election is won by the member with the simple majority of votes. The member that wins an election is always the one with the most recent log records. In the case of a tie, the member with the highest priority wins.
Rejoining cluster after shutdown for an extended period	If the server that needs to rejoin the cluster has been down for more than 24 hours, perform a hot backup on the host running the master database and restore the backup to the server that is down before restarting it. This avoids the potentially high cost synchronizing the server with the master during startup.

2

Session Delivery Manager Application Overview

Oracle Communications Session Delivery Manager is a network element management system that can be accessed through a graphical user interface (GUI), REST API interface, or SOAP API interface.

Once SDM is installed, you can access the following sliders:

> **Note:**
>
> Other sliders, such as the Device Manager, Configuration Manager, Performance Manager, and so on, will not be seen until you install a product plug-in.

- **Device Manager**—Use this slider to configure device groups. The functionality of this slider is dependant on the product plug-in(s) that you have installed.
- **Security Manager**—Use this slider to configure any security privileges that are specific to Oracle Communications Session Delivery Manager and the Oracle Communications Session Delivery Manager product plugin.
- **Fault Manager**—View events, alarms, and trap summary data.

Session Delivery Manager Product Plugin Service

A product plugin is used to activate fault, configuration, accounting, performance, and security (FCAPS) in Oracle Communications Session Delivery Manager. For example, the Session Delivery (SD) product plugin activates Oracle Communications Session Element Manager in SDM for session delivery devices, such as the Oracle Communications Session Border Controller (SBC).

SDM has limited functionality until a plugin is uploaded and installed in SDM. Product functionality activated by the plugin in the SDM GUI is specific to what the plugin supports. For example, if you see a drop-down menu, field or checkbox that cannot be accessed, the plugin does not support this functionality in the GUI.

Use the plugin service in Oracle Communications Session Delivery Manager to install the product plugin, which provides different sliders depending on the instructions contained in the product plugin. For example, the **Dashboard Manager**, **Configuration Manager**, **Performance Manager**, **Report Manager**, and **Route Manager** sliders appear once the SD plug-in is installed. See the product plug-in documentation for more information about supported sliders.

More than one product plugin can be installed on SDM at the same time, and the functionality of the plugin(s) is propagated to other SDM nodes in a clustered environment. The following example shows how the SD and Enterprise product plugins provide their respective devices access to Session Element Manager, Report Manager and Route Manager.
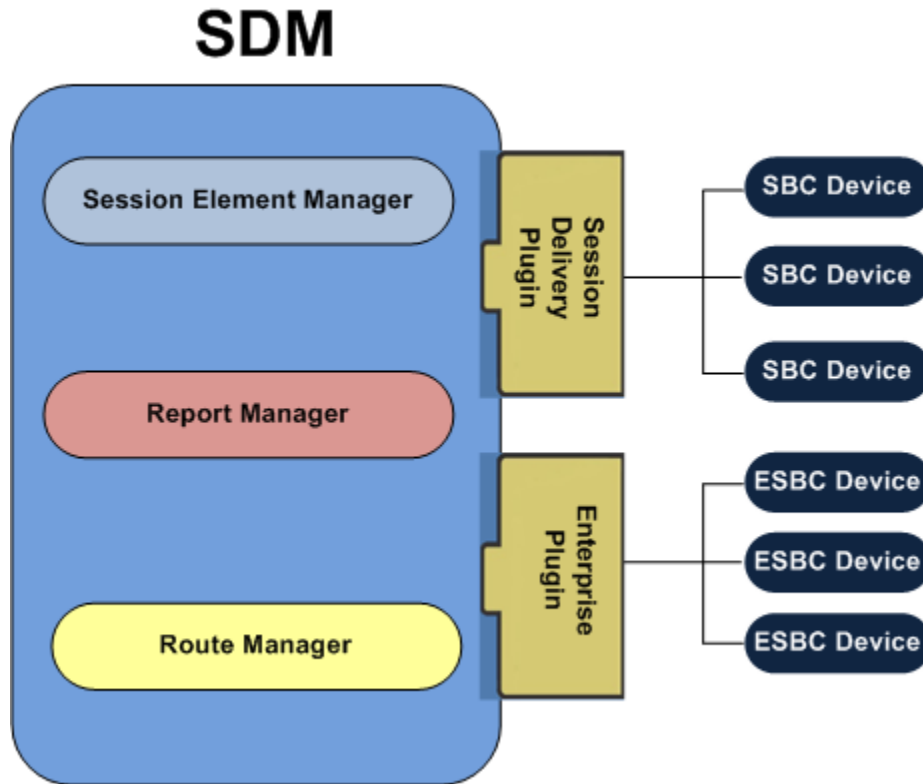
Log Into Session Delivery Manager

1. Open your Web browser and connect to the SDM server through your web browser using one of the following address formats (depending how you installed the SDM web server):

   HTTP (unsecured) session:

   ```
   http://<SDM server IP address>:8080
   ```

   HTTPS (secured) session:

   ```
   https://<SDM server IP address>:8443
   ```

   > **Note:**
   >
   > We recommend that during the installation, you select HTTPS as the system running mode so that your system can create secure connections over the network.

2. In the login page, enter the appropriate user name and password and click **Login**.

   The SDM GUI appears.

Access Session Delivery Manager GUI Elements

The following figure shows the main SDM GUI elements:

Figure 2-1   SDM GUI
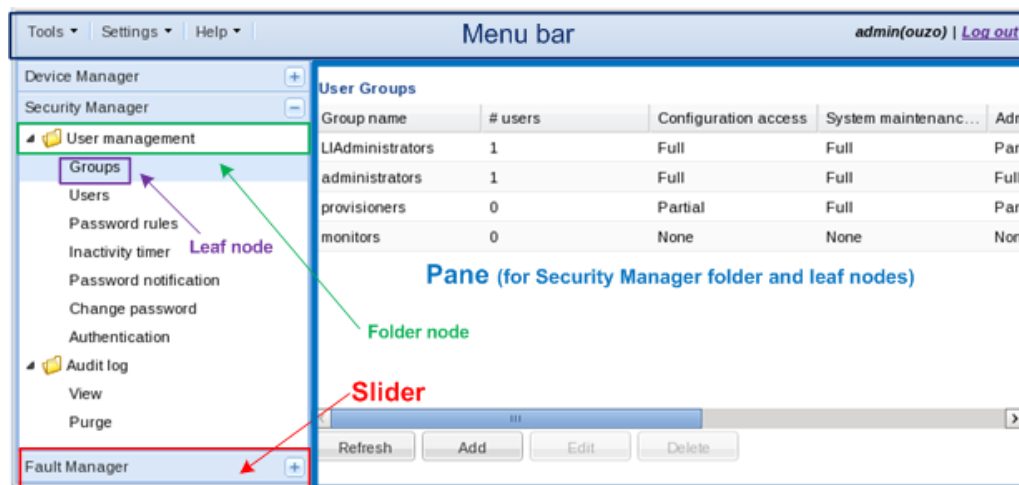
- **Menu bar**—Use this GUI element to access features on the **Tools**, **Settings**, and **Help** menus.

- **Slider**—Access Session Element Manager FCAPS applications: Dashboard Manager, Device Manager, Security Manager, Configuration Manager, Fault Manager, Performance Manager and the Report Manager and Route Manager applications. If you are installing SDM for the first time, the **Device Manager**, **Security Manager**, **Fault Manager** sliders appear only before any plugins are installed.

- **Folder node**—Use this node to access slider leaf nodes.

- **Leaf node**—Use this node to access slider application features.

- **Pane**—The place where slider application features are viewed, accessed, and configured.

Tools Menu

Use the **Tools** menu to access the following selections:

- **Passwords**—Change the password you used to login to the SDM GUI. Refer to the Change Your User Password section in this chapter for more information.

- **Health Monitor**—View the health of each SDM system. Refer to the Monitor Session Delivery Manager Server Health and Disk Usage chapter for more information.

- **Upload configuration schema file**— A configuration schema provides a configuration model and information for a device. Refer to the *Configuration Manager* chapter in your Oracle Communications Session Element Manager User Guide plugin product documentation for more information about uploading a configuration schema file for a device.

- **Server Diagnostics**—Use this selection to view SDM server log information including how log data is collected. Refer to the Use Server Diagnostic Logs section for more information.

- **Device association information**—Use this selection to see how many devices are in use by the product plugin and its associated applications.

- **Certificates**—The SDM server can use trusted certificates (certificates validated by a CA or self-signed certificate) in its trust store. Refer to the Manage Transport Layer Security Certificates chapter for more information.

- **Plugin Management**— Upload and install a plugin product application, such as an element manager (EM). Refer to the Manage Product Plug-ins chapter for more information.

Settings Menu

Use the **Settings** menu to access the following selections:

- **Faults**—Configure faults, fault notifications, trap receivers and heartbeat traps.

- **Alarms**—Configure audible alarms, alarm colors, and configure how alarms are displayed in SDM.

- **Edit Login Banner**—If you have full administrative privileges, you can define the informational banner seen when a user logs into SDM. This banner can also be specified to contain a user compliance rule with terms and conditions regarding the use of the application.

Help Menu

1. Select **Help** > **Help topics**.

2. In the web page that displays for your plugin, select from the following default document links if SDM installed only:

   - *Session Delivery Manager Administration Guide*

   - *Session Delivery Manager Security Guide*

   If you have installed a product plugin, select its link under the **Oracle Communications Plugin Help** title. A web page displays for the product plugin and its documentation links.

   Select **Help** > **About** to get SDM system and product plugin information (if it is installed) in a pop-up window.

Customize the Display

Depending on the features that you use in the SDM GUI, you can change the way information is displayed by customizing the way table columns are displayed and table entries are ordered. You can also customize the number of records that are displayed per page. Any customization that you do is maintained for the life of the session only. Once you log out, the changes that you made, revert to their default state.

1. Position the cursor over a column heading. An arrow appears on the right hand side of the box. For example:

2. Click the down arrow to display the menu. For example:

3. Select **Sort Ascending** to sort the data in ascending order or **Sort Descending** to sort the data in descending order.

4. Select **Columns** to access a list of column names. For example:

☑ Device
☑ Target Name
☑ Software Version
☑ Hardware Version
☑ Group/Cluster
☐ SBI TLS Status
☐ Primary Serial Num
☐ Secondary Serial Num
☐ Object ID
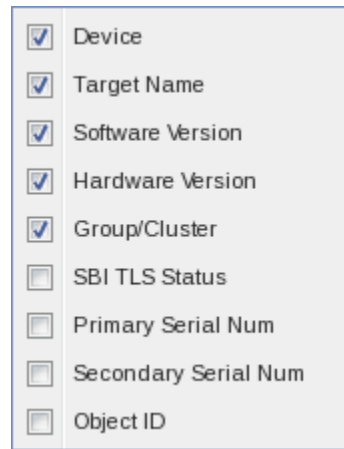
5. Click a marked checkbox to hide that column or click to check an empty checkbox to display that column. The display view automatically updates.

6. To display a page of records that you want to view, you can use the buttons to move between pages or enter the page number you want.

7. To customize the number of records that are displayed per page, click the **Size** drop-down list.

> **Note:**
>
> If you cannot sort table columns using the **Sort Ascending** or **Descending** column options, select the **All** option from the **Size** drop-down list in order to use these column options. For example, the **All** option appears in the **Size** drop-down list when you load a device in Configuration Manager to display records for the **local-policy** configuration element. If you are having trouble sorting the column order for this configuration element, use the **All** option and try again.

Page [1] of 1 Size [All ▾]
-time   Description   10
                       15
                       20
                       25
                       50
                       100
                       All
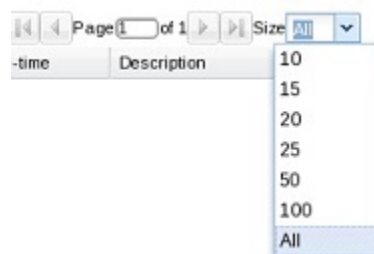
8. Click elsewhere in the display to clear the menus.

Get Help Tips for Fields and Menus

You can find various help tips for fields and menus that appear in the GUI by placing your mouse arrow over a field or attribute name to make a help tip appear. For example:
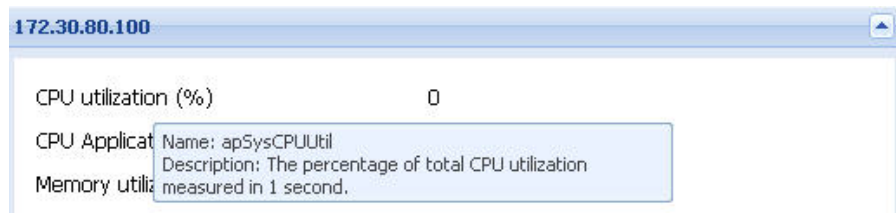
Change Your User Password

Use this task if you want to change the password that you used to login to the Oracle Communications Session Delivery Manager GUI.

1. On the menu bar, select **Tools** > **Passwords** > **Change user password**.

2. In the Change password dialog, complete the following fields:

Name	Description
Current login user password	The current user password used to login.
New password	The new password.
Confirm new password	The new password.

3. Click **OK**

Use Server Diagnostic Logs

You can view or retrieve and download various Oracle Communications Session Delivery Manager server logs to your local system and configure the granularity and what type of information is displayed for a particular log level.

Configure Log Levels

You can configure log severity levels to filter the granularity of information presented in logs.

1. On the menu bar, select **Tools**, **Server Diagnostics**.

2. In the **Summary** pane, click the **Log Levels** tab.

3. In the **Logging Levels** section, select **All Files** (default) or **Per Individual File** to choose the granularity for how files are logged.

4. If you selected **All Files**, select from the following log levels in the **Log Level** drop-down list.

DEBUG	Debugging, informational, warning, and error logs are included.
TRACE	Trace, informational, warning, and error logs are included.
INFO	(Default) Informational, warning, and error logs are included.
WARN	Warning, and error logs are included.
ERROR	Error condition logs.

5. If you selected **Per Individual File**, select a log level (refer to the previous step) for each log type that is retrieved. You can select **Refresh** to go back to the saved log file levels.

6. Click **Apply** for your logging level changes to be applied.

> **Note:**
>
> If the SDM restarts, all logging levels are reset back to the default (**INFO**).

Retrieve and Download Logs

Use this task to collect and download an NNC system tar file to your local client that contains logs for various databases, server processes, product plug-ins and server applications (such as for the HTTP/HTTPS server) running on SDM cluster node(s).

1. On the menu bar, select **Tools**, **Server Diagnostics**.

2. In the **Summary** pane, click the **Log Retrieval** tab.

3. In the **Include/Exclude extra information** section, you can include or exclude information contained in the log you are retrieving by selecting from the following options:

Berkeley Database checkbox	This checkbox is unchecked by default. Check the checkbox to include Berkeley database information that provides database storage for SDM user name and user group variable information in the logs that you receive.
Discovery Folder checkbox	This checkbox is unchecked by default. Check the checkbox to include device configuration information from the dataDoc.gz file that is in the Discovery folder, in the logs that you receive.

4. View the following collection information in the **Collection Information** section:

Most Recent Collection Date field	This field displays the last time logs were collected, so that you can determine if there is no collected log file in the system.
Collected File Name field	The directory, including the collected file name. For example: /opt/AcmePacket/NNCArchive/ NncDiagnosticsArchive/nncinfo.tar

5. View the following **Collection Status** table information:

Server column	The SDM cluster node.
Collection status column	The following cluster node retrieval statuses are available: • In progress—The file is downloading. • Succeeded—The files were retrieved from a specific node and sent to the node from which the collection was initiated successfully. • Failed—The file failed to download.
Object ID column	(Hidden) Internal database object ID.

6. Click **Start Collection** to collect the server files on each SDM cluster server node.

You can click the **Refresh** button to refresh the status of the retrieval process.

7. Once all servers have finished the collection process (the **Collection Status** column for each server displays either a **Succeeded** or **Failed** status), click **Download now** to get the log files from server nodes that have successfully collected log data.

8. In the next dialog box that appears, select **Save File** to save the tar file that is compiled to your default download location on your client and click **OK** or click the **Open with** option to open the log file to view its contents.

3

Manage Product Plug-ins

Use this chapter to perform a variety of SDM product plug-in management tasks.

Plugin Tasks

Use the following tasks to perform product plugin actions in Oracle Communications Session Delivery Manager.

The following figure shows the life cycle of a plugin.

Figure 3-1   Plugin life cycle
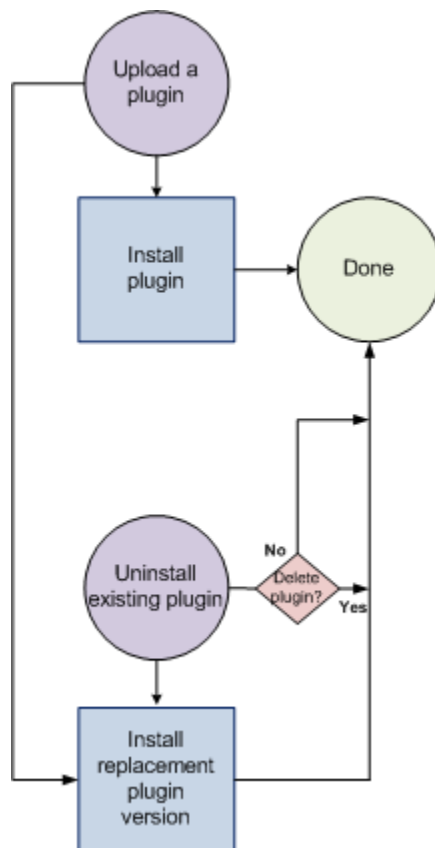
When you perform upload, install, uninstall, replace, and delete plugin actions on one node, the other nodes of the cluster are signaled to apply the same action. All users who are logged into a node, other than the one where the action was initiated, should refresh their browser to have their GUI updated for the new functionality. If some functionality is still not available, re-login to the node.

Upload a Plugin

Use this task to upload your product plugin from the system where your software distribution media containing the product plugin is kept to SDM.

> **Note:**
>
> If you have upgraded from a previous version of SDM, the (element manager) product plugin that manages your devices is uploaded and installed automatically on your system and appears on the **Plugin Management Tool** pane in the **Element Manager Plugins** table. If you installed SDM for the first time, no product plugins appear in the table.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Plugin Management Tool** pane, click **Upload**.

3. In the **Upload Plugin** dialog box, click **Browse** to navigate to the directory on your system where you keep the product plugin software package to upload to SDM.

   For example:

   ```
   sd1.0_Package.zip
   ```

4. In the **Upload Plugin** dialog box, click **Upload**.

   A dialog box displays showing the upload was successful and the plugin appears in the **Element Manager Plugins** table in the **EM** (element manager) tab.

Install a Plugin

Use this task to install the product plugin in SDM.

> **Note:**
>
> One version only of a plugin can be installed at a time.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Element Manager Plugins** table, select the plugin row and click **Install**.

3. In the plugin installation dialog box, click **Yes** to continue the product plugin installation. Your installed plugin contains instructions that initiate core features and functionality in SDM. This results in new functionality displaying in existing sliders and new sliders appearing in SDM.

4. If the dialog box shows that the installation failed, you are prompted to resolve the identified problem. Once the problem is fixed, click **Recover** to put the system into a state where another installation of the plugin can be attempted.

Uninstall a Plugin

When a plugin is uninstalled, it is out of service. SDM loses the ability to manage the network functions (NF) and their respective devices that are dependent on this plugin. For example, configuration, polling, trap processing, device statistic gathering, and so on are suspended. However, the devices themselves continue to operate normally on the network.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Element Manager Plugins** table, select the installed plugin row and click **Uninstall**.

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

4. In the success dialog box, click **OK**.

> **Note:**
>
> The plugin continues to be listed in the **Element Manager Plugins** table on the **EM** tab. The **Status** column shows the state of the plugin as **UNINSTALLED** and the functionality of that plugin ceases. For example, sliders, folder and leaf nodes may disappear and fields, drop down lists, and so on may disappear from functionality that remains.

5. If the dialog box shows that the plugin failed to uninstall, you are prompted to resolve the identified problem if applicable. Once any applicable error(s) are fixed, click **Recover** until it is successfully uninstalled.

You can now choose to install a new product plugin, new version of a product plugin, or install a previous version of a product plugin.

Replace a Plugin

You can replace an existing product plugin to a different version of the same product plugin.

SDM service continues for plugin network functions (NF) and their respective devices when the replacement version of the plugin is installed successfully.

> **Note:**
>
> More than one version of a plugin can be uploaded to SDM.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Element Manager Plugins** table, select the plugin row and click **Install**.

> **Note:**
>
> A warning appears that this process suspends SDM service for any devices associated with the plugin.

3. In the dialog box that appears, click **Yes** to continue the product plugin installation.

ORACLE

A dialog box displays the successful replacement of the plugin and all affected services return to operation. If there are any NFs that are no longer supported by the installed plugin, all devices belonging to these NFs are marked as unmanageable and can be removed by the system administrator manually.

4. If the dialog box shows that the replacement of the plugin failed, you are prompted to resolve the identified problem if applicable. Once any applicable error(s) are fixed, click **Recover** to put the system into a state where another installation of the plugin can be attempted.

Delete a Plugin

When you delete a product plugin from the **Element Manager Plugins** table, the product plugin .zip file that exists on the SDM server is deleted.

> **Note:**
>
> You can delete a plugin from SDM only after you uninstall the plugin first. See the Uninstall a Plugin section for more information.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Element Manager Plugins** table, select the uninstalled plugin row and click **Delete**.

   The following options are presented, depending on whether or not other uninstalled versions of a plugin are present:

   • If you are deleting the last remaining version of an uninstalled product plugin, the following confirmation dialog box appears:
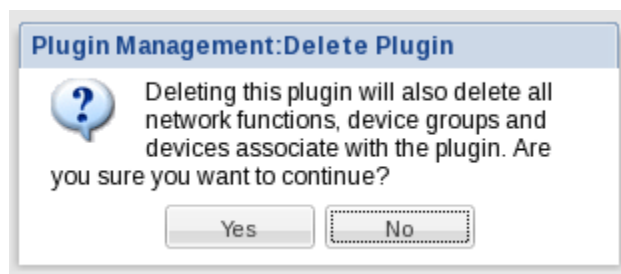
   • If you are deleting one plugin version among others, a confirmation dialog box appears with the following options:

     – Check the **Clean up NFs** checkbox to remove network functions (NFs) and any devices associated with the plugin from SDM.

     – Check the **Clean up file system** checkbox to clean the plugin directory on the SDM server. For example:

       ```
       AcmePacket/NNCArchive/pluginArchive/<pluginVendorProduct>/
       <pluginName>/temp
       ```

3. Click **Yes** in the confirmation dialog box to complete the deletion of the plugin.

4. In the success dialog box, click **OK**.

> ✏ **Note:**
>
> If the plugin displays a **Failed_Delete** status, the system prompts you to confirm the deletion of the plugin to force its deletion.

The plugin is no longer listed in the **Element Manager Plugins** table on the **EM** tab.

View Plugin Information

Use this section to view status information for your plugin during installation.

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Plugin Management Tool** pane, you can view plugin information in the following columns displayed in the **Element Manager Plugins** table on the **EM** tab:

Name	Description
Name	The name of the plugin.
Status	Plugin states: • **INSTALLED**—The plugin is successfully installed. • **UPLOADED**—The plugin is successfully uploaded. • **UNINSTALLED**—The plugin is successfully uninstalled. Failed plugin states: • **FAILED UPLOAD**—The plugin failed to upload from your local directory. • **FAILED INSTALL**—Check if there is an installed plugin with the same plugin Name, Vendor, Product, and version. Errors may also have occurred during the installation. • **FAILED UNINSTALL**—This message may display when uninstalling the previous version of a plugin and errors occur because the database service is temporarily down, the file system is busy, network system is down, and so on. • **FAILED DELETE**—The plugin failed to be removed.
Server	The IP address of the SDM server on which the plugin is installed.
Version	The version of the plugin.
Vendor	The company that developed the plugin.
Product	The product name of the plugin.
Description	The description of the plugin specified by the system administrator.
Package Name	The full SDM server directory on which the plugin package is installed.
Date Modified	The date on which the plugin was last modified. For example, this can be its install date, the date the plugin was uploaded, and so on.

Name	Description
Object ID	(Hidden) The internal SDM object ID item.
pluginType	(Hidden) The type of plugin that allows communication to network elements.

The following **Element Manager Plugins** table shows an example of a cluster installation with two-nodes. Two versions of the session delivery (SD) plugin exist (v1.0. and v2.0), and only one version is installed at a time. This example also shows how the plugin status can become unsynchronized across the nodes of a cluster in the case of the EnterpriseExt plugin where the delete action is processed on 10.196.65.3 SDM server node, but not completed yet on the 10.196.65.19 SDM server node.

Element Manager Plugins (Search Criteria:All)

Refresh   Search   Show All   Viewing 1-8 of 8   Page 1 of 1

Name	Status	Server	Version	Vendor	Product	Package Name
AcmeSD	UNINSTALLED	10.196.65.3	1.0	Oracle	Session Delivery	sd1.0_Package.zip
AcmeSD	UNINSTALLED	10.196.65.19	1.0	Oracle	Session Delivery	sd1.0_Package.zip
Enterprise	UPLOADED	10.196.65.3	1.0	Oracle	ESBC/ECB	enterprise1.0_Pack...
Enterprise	UPLOADED	10.196.65.19	1.0	Oracle	ESBC/ECB	enterprise1.0_Pack...
EnterpriseExt	DELETED	10.196.65.3	1.0	Oracle	ISR/EOM	enterpriseext1.0_Pa...
EnterpriseExt	UPLOADED	10.196.65.19	1.0	Oracle	ISR/EOM	enterpriseext1.0_Pa...
AcmeSD	INSTALLED	10.196.65.3	2.0	Oracle	Session Delivery	sd2.0_Package.zip
AcmeSD	INSTALLED	10.196.65.19	2.0	Oracle	Session Delivery	sd2.0_Package.zip

Edit the Plugin Description

1. On the menu bar, select **Tools** > **Plugin Management**

2. In the **Plugin Management Tool** pane, click **Edit**.

3. In the **Plugin Management Edit Plugin** dialog box, change, add or remove a description in the **Plugin Description** field.

4. Click **Update**.

4

Security Manager

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

- Create and manage users.
- Create and manage 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.

Figure 4-1   Security Manager Slider Parameters
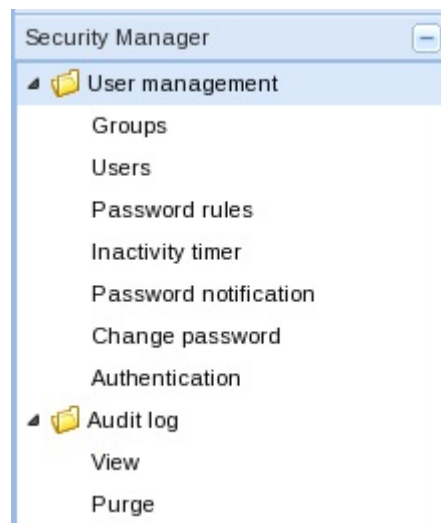
Configure User Groups

A user group is a logical collection of users grouped together to access common information or perform similar tasks in SDM. The default **LIAdministrators**, **administrators**, **provisioners**, and **monitor** user groups are provided in SDM for you, or you can add new user groups so that you have the flexibility to define specific privileges for them based on the unique needs of your users. You can also map a local default user group or a local user group that you add in SDM to an external domain user group provided by RADIUS or LDAP authentication so that the external group can inherit the authorization privileges of the local user group.

Add a User Group

You can add a user group to which you assign users later. Those users in turn, inherit the group-based privileges that you copy from default user groups.

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.

2. In the **User Groups** pane, click **Add** to add a new user group.

3. In the **Add Group** dialog box, complete the following fields:

Name	Description
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.
Group permissions copy from drop-down list	Choose from the following default user groups to copy their privileges: • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure SDM and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure SDM, and has the fewest privileges.

4. Click **OK**.

5. In the success dialog box, click **OK**.

6. Click **Back** to return to the **User Groups** table.

Delete a User Group

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.

2. In the **Groups** pane, 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 application products. For the default **LIAdministrators**, **administrators**, **provisioners**, and **monitor** user groups, only device group privileges can be changed.

> ✎ **Note:**
>
> All user group privileges that are available through SDM are described in the following sections. You may not see some of these user group privileges in the **Configuration**, **Device maintenance**, **Administrative operations**, **Fault management**, **Device groups**, and **Applications** tabs in SDM until you install your product plugin.

Apply User Group Privileges for Configuration

1. Expand the **Security Manager** slider and choose **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.

Name	Description
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 **Device 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 LI item	Set privilege levels for lawful intercept features.
Configure system item	Set privilege levels for the configuration of system usage parameters.
Route Manager Central Configuration folder	See the *Oracle® Communications Route Manager User Guide for Session Delivery Products* for more information about privileges that you specify in this folder.

Name	Description
Work order folder	Set privilege levels for all of the following user management operations accessible for the configuration of work orders.
Create work order item	Set privilege levels for creating a work order.
Execute work order item	Set privilege levels for executing a work order.
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 levels for viewing a configuration.
Entitlements item	Set privilege levels for viewing license details for an NF device.
Update to device folder	Set privilege levels for the following device configuration operation items in this folder.
Save configuration item	Set privilege levels for saving the configuration of a device.
Save and activate configuration item	Set privilege levels for saving and activating the configuration of a device.
Activate configuration item	Set privilege levels for activating the configuration of a device.
Configuration archive folder	Set privilege levels for all of the following configuration archive operations.
Back up configurations item	Set privilege levels for backing up configurations in the configuration archive.
Restore configurations item	Set privilege levels for restoring configurations in the configuration archive.
Delete archived configurations item	Set privilege levels for deleting 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 slider 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 options:

   • **Full**—The user group is allowed to reboot a device.

   • **None**—The user group is not allowed to reboot a device.

6. Click **Apply**.

Apply User Group Privileges for the Administrative Operations

1. Expand the **Security Manager** slider and choose **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.

   • **View**—Allowed to monitor only.

Name	Description
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 folder	Set privilege levels for all group item operations.
Add group item	Set privilege levels to add a new device group.
Update group item	Modify groups.
Delete group item	Delete existing groups.
User operations folder	Set privilege levels for all the following user operations accessible on the **Security Manager** slider.
Add users item	Create new users.
Update users item	Modify user information.
Delete users folder	Delete existing users.
Reset password item	Reset the password for a user who needs to login to **Oracle Communications Report Manager**.
Change password item	Change another user's password used to login to **Oracle Communications Report Manager**.
Change inactivity timer item	Change the inactivity timer, which logs off the user if the client is no longer being used.
Change Password Rule item	Configure the password rules used when creating a new user.
Edit login banner	Edit the login banner for users logging into **Oracle Communications Report Manager**.
Password notification	Change the notification interval.
Device group folder	Assign privilege for all functions pertaining to a device group (see below).
Add device group item	Set privilege levels to add a new network function containing a device group for either device(s) or a device cluster.
Delete device group item	Delete a device group.
Move device group item	Move a device group.
Rename device group item	Rename a device group.
Device folder	Assign privilege to all of the following device operations accessible through the **Device Manager** and **Configuration Manager** sliders.
Activate device	Activate a new device.
Add device item	Add a new device.
Remove device item	Remove an existing device.
Move device item	Move a device.

Name	Description
KPI Operation item	Set privilege levels to get device KPIs, register KPIs, deregister KPIs, or update registered KPIs.
Edit login banner item	Allow users of a group to change the informational banner seen when a user logs into SDM.
Change password message interval item	Send alert that prompts user to change their password a certain number of days before their password expires.
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.
View health monitor console item	Access health monitor console to detect issues.
Change configuration archive settings item	Change configuration archive settings.
Update OS/System account password item	Update the operating system and the system account password.
Authentication item	Update authentication parameters.
Server Diagnostics item	Access to server diagnostics.

6. Click **Apply**.

Apply User Group Privileges for Fault Management Operations

An element manager system (EMS) must be licensed to apply user-group privileges for fault management operations that apply to the events and alarms that appear on the **Fault Manager** slider.

1. Expand the **Security Manager** slider and choose **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.

Name	Description
Fault management folder	If the **None** privilege is chosen, the **Fault Manager** slider does not appear in the SDM GUI.
Events and Alarms folder	Assign the privileges for all of the following event and alarm operations accessible on the **Fault Manager** slider.
Alarms folder	Assign the privileges for all of the following alarm operations accessible on the **Fault Manager** slider.

Name	Description
Set email notification item	Create an email list for alarms.
Delete alarm item	Delete alarms.
Remap severities item	Edit the alarm severity levels.
Events folder	Assign the privileges for all of the following event operations accessible on the **Fault Manager** slider.
Delete events item	Delete events.
Configure trap receiver item	Assign privileges to configure a trap receiver.

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:

Name	Description
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.
Home item	(Default device group) In the **Privileges** column drop-down list, choose the following user group privilege options for items in the **Device groups** box table described below: • **Full**—(Default) Allowed to perform device group operations. • **None**—Users do not have authorization to the device group. • **View**—Users can view the group on the **Device Manager** slider, but cannot perform any operations such as adding or deleting a child group.

The **Preview** box displays the device group based on the privileges that are assigned (**Full**, **View**).

5. Repeat the previous step for other device groups (if there are any).

6. Click **Apply**.

Apply User Group Privileges for Route Manager

Use this task to apply user-group privileges for Oracle Communications Session Delivery Manager configurations.

Depending on your user privileges in Oracle Communications Session Delivery Manager, you can enable privileges to configure route set groups and templates, perform backups or restore route sets, and perform route set operations on devices.

1. On the navigation bar, select **Security Manager** > **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 expand the **Route Management Central** configuration folder and expand it to expose the following folder items:

Name	Description
Configure route set item	Click this item row to activate the **Privileges** drop-down list to do the following operations: • Select **Full** to enable the **Route Sets**, **Route Search**, and **Route Set Compare** tabs to appear. These tabs are used to add, configure and manage route sets, and retrieve LRT files. • Select **View** to view the route set configuration only. • Select **None** to disable route set operations and make them disappear from the GUI.
Configure templates item	Click this item row to activate the **Privileges** drop-down list to do the following operations: • Select **Full** to enable the **Import Template** tab. This tab is used to configure the templates that are used to map CSV file columns to route properties, and import CSV files. • Select **View** to view configuration templates only. • Select **None** to disable template operations and make them disappear from the GUI.
Backup/Restore item	Click this item row to activate the **Privileges** drop-down list to do the following operations: • Select **Full** to enable the **Route Set Backups** and **Route Set Scheduled Backups** tabs. These tabs are used to create backup files of the route set(s) and restore the backup files to the device. • Select **View** to view backup files of the route set(s) only. • Select **None** to disable backup operations and make them disappear from the GUI.
Device operation item	Click this item row to activate the **Privileges** drop-down list to do the following operations: • Select **Full** to enable the **Device Route Sets**, **Associated Devices**, **Device Route Set Updates**, and **Update Task History** tabs. These tabs are used to add route sets to devices, view the route sets associated with each device, update route sets, and update task histories. • Select **View** to view route set device information only. • Select **None** to disable route set device operations and make them disappear from the GUI.

4. Click **Apply**.

Apply User Group Privileges for Applications

1. Expand the **Security Manager** slider and choose **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 **Applications** tab and click to expand the **Applications** folder.

4. Select any folder or folder item row that are described in the table below that you want to modify and click the **Privileges** column to activate the drop-down list.

Select the following privilege from the **Privileges** drop-down list:

- **Full**—Enable GUI elements (such as tabs) to perform configuration operations.

- **View**—View information only.

- **None**—Disable configuration operations and make them disappear from the GUI.

> **Note:**
>
> You must set the **Execute Reports** item privilege level to **Full**. See the table below for more information.

Name	Description
Application folder	Set privilege levels for all application operations.
Report Manager folder	Set privilege levels for all reporting operations accessible on the **Report Manager** slider.
Execute Reports item	You must set the privilege level for users belonging to a group to run reports full privileges so that collection reports can be configured.
Administration folder	Set all administration privileges for **Oracle Communications Report Manager**.
Configure Retention Policy item	Set privilege levels for a user group to create a retention policy for retaining Historical Data Recording (HDR) data over a period of time.
Register BI Publisher item	Set privilege levels for the **Oracle Communications Report Manager** to register with the **Oracle Communications Session Delivery Manager** before creating and running reports.
Plugin Management folder	Set administrative privileges for plugin management.
Actions item	Set plugin action privileges for a user assigned to the Plugin Management group to perform upload, install, uninstall, edit, delete, and recover actions.

5. Click **Apply**.

Configure Users

A user is a person who logs into the system to perform application-related operations. Before this user can access any operations, they must be added to a user group. Each user group has a defined set of privileges. The operations that a user can do depends on the privileges of the user group to which the user belongs.

The following users are created by default when SDM is installed:

- **admin**—Inherits the privileges from the **administrators** group.

- **LIadmin**—Inherits the privileges from the **LIadministrators** group.

Users (other than the default users) are created, added, and given the privileges of the user groups to which they are assigned so that they can access SDM.

Add a User

1. Expand the **Security Manager** slider and choose **User Management** > **Users**.

2. In the **Users** pane, click **Add**.

3. In the **Add User** dialog box, complete the following fields:

Name	Description
Group **Assigned group** drop-down list	Choose from the following pre-existing user groups: • **administrators**—This super user group privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.
User information **User name** field	The name of the user using the following guidelines: • Use a minimum of 3 characters and maximum of 50 characters. • The name must start with an alphabetical character. • The use of alphanumeric characters, hyphens, and underscores are allowed. • The name is case insensitive. • The name cannot be the same as an existing group name.
User information **Password** field	The password is entered for this user using the following password rules guidelines: • The password must be at least 8 characters long. • Use at least one numeric character from 0 to 9 in the password. • Use at least one alphabetic character from the English language alphabet in the password. • Special characters include {, |, }, ~, [, \,], ^, _, ', :, ;, <, =, >, ?, !, ", #, $, %, &, `, (,), *, +, ,, -, ., and /
User information **Confirm password** field	The same password entered again to confirm it.
User account expiration dates **Account** field	Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires.

> **Note:**
>
> If the check box is checked (default) the user account never expires.

Name	Description
Password expiration dates **Password** field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires.

> **Note:**
>
> If the check box is checked (default) the password never expires.

4. Click **OK**.

The following information displays in the **Users** table:

Name	Description
User name column	The user name.
Group column	The user group to which the user belongs.
Status column	The status of the user account is either **enabled** or **disabled**.
Operation status field	The state of the user account and its expiration date: • **active**—The account is valid and the user can log in. Neither the account nor password expiration dates have been exceeded. • **account expired**—The account expiration date has expired. • **password expired**—The password expiration date has expired. • **password deactivated**—The failed login attempts by the user exceeded the allowed number of tries as specified by the value set for password reuse count parameter in password rules. • **locked out**—The user has exceeded the login failures and the account is disabled until the lockout duration has passed.

Edit a User

1. Expand the **Security Manager** slider and select **User Management** > **Users**.

2. In the **Users** pane, select a user and click **Edit**.

3. In the **User** tab , change the following fields:

Name	Description
Assigned group drop-down list	You can change a user group that you created or one of the four default groups: • **administrators**—This super user group privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure SDM and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure SDM, and has the fewest privileges.
User status **Administrative status** drop-down list	Select either **enabled** or **disabled** as the user status.
Expiration dates **Account** field	Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires. **Note:** If the check box is checked (default) the user account never expires.
Expiration dates **Password** field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires. **Note:** If the check box is checked (default) the password never expires.

4. Click **Apply**.

Reactivate a User

A user can be denied access to SDM if the user is disabled, expired, the user password expired, or the user logs in more times (due to failed log in attempts) than is allowed by the maximum login fail attempts value.

You can reactivate a user by editing the user profile to reset the status of the user to enable, then reset the expiration in days for the account and password parameters. You can also delete the expired user and recreate the user.

The following table lists the possible causes for user deactivation and how to reactivate the user.

Cause	Action
User expired	Reset the calendar to a new date.
Password expired	Reset the password calendar to a new date.
Password deactivated	Reactivate the user account by: • Changing the user password if all expiration dates are still valid. • Extending the account expiration date. • Extend the password expiration date.
User disabled	Reset the user to enabled.

Delete a User

1. Expand the **Security Manager** slider and select **User management** > **Users**.

2. In the **Users** pane, select a user and click **Delete**.

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

4. In the success dialog box, click **OK**.

   The user name is removed from the **Users** table.

Reset a User Password

Pre-requisites: You must have the proper permissions to reset passwords.

1. Expand the **Security Manager** slider and select **User management** > **Users**.

2. In the **Users** pane, click a user from the table and click **Reset Password**.

3. In the **Reset password** dialog box, enter a new password for the user in the field provided.

4. The dialog box indicates if you entered the new password successfully. Click **OK**.

Change a User Password

If you have administrative operations permission, you can change the password of a user.

1. Expand the **Security Manager** slider and select **User Management** > **Users**.

2. In the **Users** pane, click a user from the table and click **Change Password**.

3. In the **Change password** dialog box, complete the following fields:

Name	Description
Enter your password field	Enter the password of the logged in user.
Enter new password for user field	The new password for the user.
Confirm new password for user field	The new password is entered again to confirm it.

4. Click **OK**.

Change User Password Rules

Use this task to change the password rules that specify the length of the password, how many times it can be reused, and whether specific characters, such as a numeric value, can be used.

1.   Expand the **Security Manager** slider and select **User management** > **Password rules**.

2.   In the password rules pane, complete the following fields:

Name	Description
Maximum login fail attempts **For administrator users** and **For non-administrator users** fields	The value that indicates the maximum login attempts allowed before the user is locked out of the system. You can set a different value for both administrator users and non-administrator users. The default value is 5 attempts.
Account lockout duration **For administrator users (minutes)** field	Enter the number of minutes that an administrator user is locked out after the maximum login fail attempts **For administrator users** value has been reached. The default is 15 minutes.

> **Note:**
>
>   This parameter applies to Administrator users only. Non-administrator users remain locked out until their login is reset.

Name	Description
Password reuse count **For all users** field	The value that indicates the number of counts to use to prevent the reuse of a password. The reuse count restricts the user from reusing the password entered in the last number of counts. For example, if you enter 2 here the user cannot reuse the same password used on the previous two occasions. You can change the password for this user by using the guidelines below.
Password length for administrator users **Minimum length** and **Maximum length** fields	The values for the minimum (no less than six characters) and maximum (up to 16 characters) length of a password for a user who has administrator privileges.
Password length for non-administrator users **Minimum length** and **Maximum length** fields	The values for the minimum (no less than six characters) and maximum (up to 16 characters) length of a password for a user who does not have administrator privileges.
Password contains at least one of the following	Check the checkbox for each of the following rules that you want to enforce: • **Numeric character**—Use at least one numeric character from 0 to 9 in the password. • **Alphabetic character**—Use at least one alphabetic character from the English language alphabet in the password. • **Special character**—You can include the following: {, |, }, ~, [, \\,], ^, _, ', :, ;, <, =, >, ?, !, ", #, $, %, &, `, (,), *, +, ,, -, ., and /

3.   Click **Apply**.

Notify When to Change the User Password

You can configure when the user is notified to change their password before it expires.

When the user logs into SDM, the system checks user credentials and the password expiry time for the user. If the password is due to expire, a warning is displayed that prompts the user to change their password.

1. Expand the **Security Manager** slider and select **User management** > **Password notification**.

2. In the **Password expiration notification** panel, enter a value in the **Days prior to password expiration** field.

3. Click **Apply**.

Configure External User Authentication

Users who belong to the external domain user group are authenticated outside of SDM by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

- A RADIUS server provides centralized Authentication, Authorization, and Auditing/ Accounting (AAA) security protocol management for users who connect and use a network service.

- An AD domain controller provides a directory service in a Windows domain type network using Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

An external domain user group must be mapped to an internal (local) user group in SDM so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group.

> **Note:**
>
> Internal and external users are both supported simultaneously. However, external users do not have corresponding stored user records or username and password information.

Determine the RADIUS Group that Your Devices are Using

If you are using a RADIUS server for external authentication and authorization, there is an additional step that you may not have completed. The RADIUS server must be configured to send a user group attribute along with its accept message. This user group attribute contains a configured group policy. The default user group attribute name is **Filter-Id**, however the RADIUS server administrator may have used a different name for the user group attribute. If the user group attribute name used on your RADIUS server is different than the commonly used default (**Filter-Id**) user group attribute, you can change the default user group attribute name in SDM in the following Configure a RADIUS Server section.

To determine the name of the user group policy that was configured on your RADIUS server that you will use later to add and map a local SDM user group to the external domain user group, use the **Test group membership** tool in SDM. See the Find an External Domain User Group section for more information.

Configure a RADIUS Server

This task is used to configure a RADIUS server domain for external user authentication.

- The RADIUS server must be configured to use the same shared secret string for all cluster nodes.

- The RADIUS server must be configured to return one or more attribute values in the authentication response message to represent the groups to which a user belongs.

1. Expand the **Security Manager** slider and select **User Management** > **Authentication**.

2. In the **External authentication** pane, select the **RADIUS** radio button and click **Add**.

   The **RADIUS** servers table becomes available for use.

3. In the **Add a radius server** pane, complete the following fields:

Name	Description
Address field	The IP address or DNS name of the RADIUS server.
Port field	This field is pre-populated with the default RADIUS server listening port **1812**. If you are using a different listening port on your RADIUS server, enter a new value.
Shared secret field	Click **Edit** next to the field. In the **Encrypted shared secret** dialog box, enter the following parameters: • **Shared secret**—The string assigned within the RADIUS server configuration to a given RADIUS client. • **Confirmed shared secret**—The same shared secret string again to confirm your input.

Name	Description
Password authentication mechanism drop-down list	**PAP** is chosen by default. The password authentication protocol (PAP) is an authentication protocol that uses a password in a point-to-point (PPP) session to validate users before allowing them to access server resources. Choose from the following options if you want to authenticate the user with another protocol: • **CHAP**—The challenge-handshake authentication protocol (CHAP) authenticates a user or network host to an authentication entity to protect against replay attacks by the peer through the use of an incrementally changing identifier and a variable challenge value. • **MSCHAPV1**—The Microsoft CHAP Version 1 (MS-CHAP v1) version of CHAP is used with RADIUS servers to authenticate wireless networks. In comparison with CHAP, MS-CHAPv1 is enabled by negotiating CHAP Algorithm 0x80 in the link control (authentication) protocol (LCP) option 3. LCP option 3 sends the Configure-Nack LCP packet type when all the LCP options are recognized, but the values of some options are not acceptable. Configure-Nack includes the offending options and their acceptable values). MS-CHAPv1 also provides an authenticator-controlled password change and authentication retry mechanisms, and defines failure codes, which are returned in the Failure packet message field. • **MSCHAPV2**—The Microsoft CHAP Version 2 (MS-CHAPv2) uses the same authentication as MS-CHAPv1, except that CHAP Algorithm 0x81 is used instead of the CHAP Algorithm 0x80. • **EAPMD5**—The extensible authentication protocol (EAP-MD5) offers minimal security and is used in wireless networks and point-to-point networks. EAP-MD5 enables a RADIUS server to authenticate a connection request by verifying an MD5 hash of a user password. The server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with the MD5 hash. • **EAPMSCHAPV2**—The protected extensible authentication protocol challenge-handshake authentication protocol (EAP-MSCHAPv2) allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory.
Group attribute name field	This field is pre-populated with the attribute **Filter-Id** by default. **Note:** Change the default value if the RADIUS server's group attribute does not match. An attribute is necessary for the device to assign a user to a RADIUS group. This RADIUS attribute connects the user name with the attribute in order to place this user in a RADIUS group. The group attribute name is configured to be included in Access-Accept message that the RADIUS server returns to this device.

4. Click **Apply**.

External users can now be authenticated by the RADIUS server. See the Add and Map a Local User Group to an External Domain User Group section of this chapter for more information.

Configure an Active Directory Domain Controller

This task is used to configure and active directory (AD) domain controller (domain server) for external user authentication.

- The Active Directory must be configured for LDAP over SSL if the Active Directory is enabled in Oracle Communications Session Delivery Manager.

- Active Directory must support version 5, if the Kerberos protocol is used.

- Each user object in your Active Directory must store the groups of each member using the **memberOf** attribute.

- Only child groups may be mapped to local groups when group nesting is in use. This limitation is due to the **memberOf** attribute not containing a recursive list of predecessors when nesting.

1. Expand the **Security Manager** slider and select **User Management** > **Authentication**.

2. In the **External authentication** pane, select the **Active directory** radio button and click **Add**.

   The **Active Directory** servers table becomes available for use.

3. In the **Add a Domain Controller** pane, complete the following fields:

Name	Description
Address field	The IP address or DNS name of the domain controller.
Domain field	The domain name for the domain controller.
LDAP Port field	The listening port number of the LDAP service. The default is 389. Use port 636 if using SSL.
Password security drop-down list	Select from the following protocols used to authenticate the user: • **Digest-MD5**—The password cipher based on RFC 2831. • **LDAP over SSL**—The SSL to encrypt all LDAP traffic. • **Kerberos**—The Kerberos protocol to authenticate the user by specifying an existing krb5.conf file containing the information needed by the Kerberos V5 library. This includes information describing the default Kerberos realm, and the location of the Kerberos key distribution centers for known realms.

4. Click **Apply**.

   External users can now be authenticated by the AD domain controller. See the *Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Find an External Domain User Group

Use the external membership tool to find the name of an external domain user group so that it can be later mapped to a local (internal) user group.

If you are using RADIUS for external authentication, you can use this tool to test external users once an external domain server is configured and returns a list of external domain user groups to which the external domain user was assigned. This makes finding the proper external domain user group names that you need to map to the local user group easier so that the external domain user group can inherit its authorization privileges. Once you find the external domain

user group you want, see the *Add and Map a Local User Group to an External Domain User Group* section of this chapter to continue.

1. Expand the **Security Manager** slider and select **User Management**, **Groups**.

2. In the **User Groups** pane, select the local group name that you are using for the external RADIUS user group (for example, MyExternalRADIUSUserGroup) and click **Edit**.

3. In the **Configuration** tab, enter the external group name (for example, Domain Users) and click **Apply and Test**.

   The **Test group membership** dialog box displays with results for the external group with a list of domain controller group names.

Figure 4-2   Example of Test Group membership results for an external group:
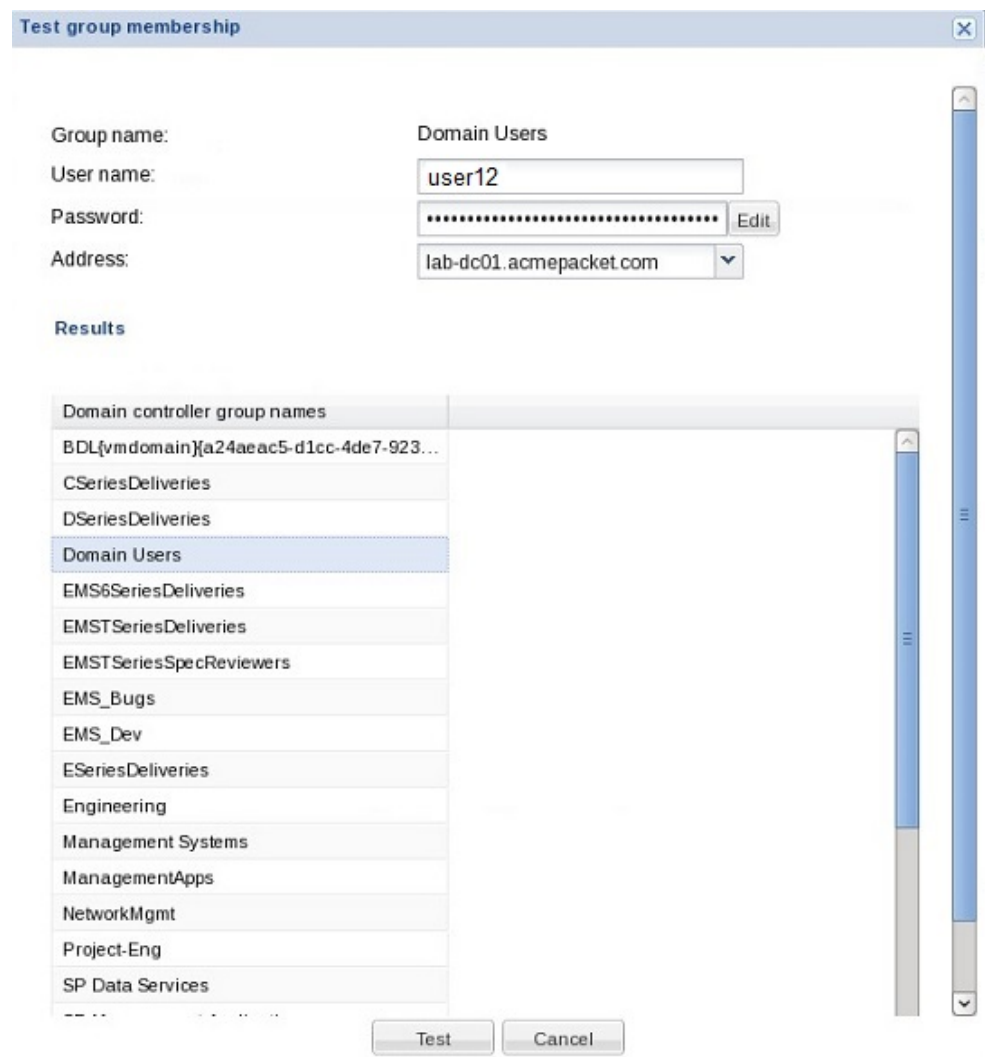
Add and Map a Local User Group to an External Domain User Group

Use this task to allow the external domain user belonging to the external domain user group to inherit the group-based authorization privileges of the local user group.

The external domain user is authenticated by a domain server, such as a RADIUS server or Active Directory domain controller. You must map the external domain user group to the local (internal) user group that was created for this purpose.

See the Find an External Domain User Group section for more information about finding the external domain user group name that you need for this task.

1. Under the **User Management** folder, select the **Groups** leaf node.

2. In the **User Groups** pane, click **Add**.

3. In the **Add Group** dialog box, complete the following fields:

Name	Description
Group name field	The local user group name that you want to use for authorization privileges. For example, **LocalUGforDomainUG**. 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.
External group name field	For Active Directory (LDAP), the external domain user group name. For example, **Domain UG**. For RADIUS, the external group name should map to attribute 11 (Filter-ID), which is in the RADIUS reply.

> **Note:**
>
> You must have at least one external domain user group entry configured on the domain server in order for this field to be displayed in the dialog box.

Name	Description
Group permissions copy from drop-down list	Choose from the following default user groups to copy their privileges: • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.

4. Click **OK**.

5. In the success dialog box, click **OK**.

6. Log out and log back into the system with the external RADIUS user to test your external connection to Oracle Communications Session Delivery Manager.

Set the Inactivity Timer to Prevent Unauthorized System Access

Oracle recommends that you set the inactivity timer to prevent unauthorized access to your system as soon as possible.

The inactivity timer logs off the user from the SDM session when its value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

> **Note:**
>
> The default inactivity timer value for an administrator is set to zero (never expire). You must choose a different value to terminate a user session after a specified time period.

1. Expand the **Security Manager** slider and select **User Management** > **Inactivity timer**.

2. In the **Session timeout** panel, complete the following fields:

Name	Description
Admin field	(Optional) The number of minutes of inactivity after which the user with administrative permissions is logged off. The range is zero to 65535 minutes. Zero sets the inactivity timer to never expire.

Name	Description
Non-Admin field	The number of minutes of inactivity after which a non-administrative user is logged off. The range is 1 to 65535 minutes. Thirty minutes of user inactivity is the default.

3. Click **Apply**.

Audit Logs

You can use the audit log (containing audit trails) generated by SDM 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 its implementation.

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 Logs

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

- 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,

Name	Description
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.

Name	Description
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.
Management Server field	(Hidden) The IP address of the management server accessed.
Client IP field	(Hidden) The IP address of the client that was used.
Description field	(Hidden) The description of the operation performed.
Sequence number field	(Hidden) The audit log reference number.

3. 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.

4. Click **OK**.

5. 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. Only the active page's entries are saved.

Search the Audit Log

1. Expand the **Security Manager** slider and select **Audit log** > **View**.

2. In the **Audit log** pane, select an entry row in the table and click **Search**.

3. In the **Audit Log Search** dialog box, complete some or all of the following fields to search the audit log:

Name	Description
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.
Management Server	The IP address of the management server accessed.
Client IP	The IP address of the client that was used.
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.

3. Click **Apply**.

Purge Audit Log Files Manually

1. Expand the **Security Manager** slider and select **Audit log** > **Purge**.

2. In the **Manual Audit log purge** dialog box, click the calendar icon next to the **Purge audit log records prior to** field and choose the date from the calendar prior to which you want audit logs purged.

3. Click **OK**.

5
Fault Manager

Fault manager is used to view events, alarms and trap event settings. Events and alarm information is based on the Oracle® standard and proprietary Management Information Bases (MIBs). All SNMP traps generated from nodes are managed by SDM.

With the introduction of Oracle Communications Session Delivery Manager, Release 8.0, network-element specific MIBs are delivered by product plugins. There are also core SDM MIBs that come with SDM.

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 can be configured in the setup application during the Typical Installation. See the *Configure Fault Management* section in the *Oracle Communications Session Delivery Manager Installation Guide* for more information.

> **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 SDM 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 SDM cluster nodes.

- Ensure that you configure northbound interface fault trap receivers on the Oracle Communications Session Delivery Manager server for northbound systems. See the Configure Northbound Interface Fault Trap Receivers chapter.

If you want more specific information about events, alarms, and MIBs that is not covered in this chapter, see the *Oracle Communications Core Session Manager MIB Reference Guide*.

Alarm and Event Configuration Tasks

The following sections describe the **Alarms** table and **Events** 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.

Manage How Alarms are Displayed

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

2. In the alarms pane, select an alarm that you want to view and click **View**.

> **Note:**
>
> Alternatively, you can double-click the alarm.

3. In the **Alarm detail** dialog box, view the following fields:

> **Note:**
>
> The following fields in the **Alarm detail** dialog box also describe the columns displayed in the alarm table in the alarms pane. The hidden fields described in this table are associated with the alarm table only.

Name	Description
Annotation	The user-defined note pertaining to this alarm.
Acknowledged by	The user that acknowledged the alarm.
Time	The date and time this alarm was generated in hours, minutes, and seconds.
Modified time	The date and time the alarm was last modified.
Description	A short description of the alarm.
Source	The exact descriptive source of the alarm.
Source IP	The IP address from which this alarm was generated.
Failed resource	The resource responsible for this alarm.
Type	The type of trap associated with this alarm as defined in the MIB. For example, TrapRelayMonitor.
System up time	Length of time the system has been operational in hours, minutes, and seconds.

Name	Description
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.

Name	Description
Trap Name	(Hidden) The exact name of the trap associated with this alarm. For example, apNNCTrapRelayAliveNotification.
Source Group ID	(Hidden) The identity of the source group associated with this alarm.
Network function	(Hidden)The network function associated with this alarm.
Object ID	(Hidden) The object identifier (OID) associated with this alarm.

Manage How Events are Displayed

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

2. Glide your mouse over a column and click the drop-down list that appears next to any column heading.

3. In the events pane, select an event that you want to view and click **View**.

> **Note:**
>
> Alternatively, you can double-click the event.

4. In the **Event detail** dialog box, view the following fields:

> **Note:**
>
> The following fields in the **Event detail** dialog box also describe the columns displayed in the events table in the events pane. The hidden fields described in this table are associated with the events table only.

Name	Description
Time (created)	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.

Name	Description
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.
Type	The type of trap associated with this event. For example, TrapRelayMonitor.
Failed resource	The resource responsible for this event.
Description	A short description of the event.
Default Severity	The system-defined severity level for this event.
Trap Category	The category to which the event belongs. For example, NNC.
System up time	Length of time the system has been operational in hours, minutes, and seconds.
Trap Name	(Hidden) The exact name of the trap associated with this event. For example, apNNCTrapRelayAliveNotification.
Source Group ID	(Hidden) The identity of the source group associated with this event.
Network function	(Hidden)The network function associated with this event.
Object ID	(Hidden) The object identifier (OID) associated with this event.

Navigate Multiple Fault Manager Pages

1. Expand the **Fault Manager** slider and choose from the following options:

   - **Events**

   - **Alarms**

2. At the top right area of the **Events** or **Alarms** pane, click the navigation icons to display the desired first page, previous page, next page, and the last page, etc.
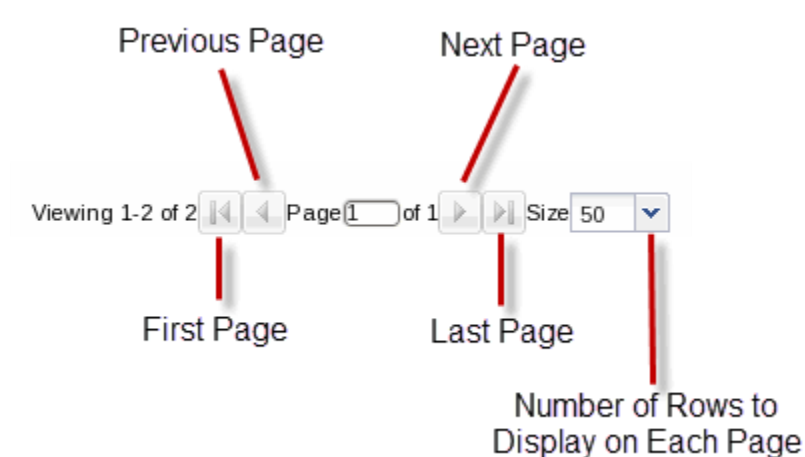
Manage the Page View for Events and Alarms

1. Expand the **Fault Manager** slider and select from the following options:

   - **Events**

   - **Alarms**

2. In the alarms or events pane, you can select from the following actions:

Name	Description
Refresh button	Click to refresh the data in the table.
Show all button	Click to show all current alarms or 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 **Filter search** dialog box, complete the following fields:

Name	Description
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).
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm.

Change the Number of Alarms or Events in a Table

1. Expand the **Fault Manager** slider and select from the following options:

   - **Events**

   - **Alarms**

2. At the top of the events or alarms pane, click the **Size** drop-down list.

   Note:

   By default, 50 table items are displayed.

3. Click the appropriate value.

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. In the events or alarms pane, click **Save to file**.

3. In the save dialog box, select either to open the file or save the file.

> **Note:**
>
> If you save the file, the file is saved to your browser's default download location.

4. Click **OK**.

Delete Alarms or Events

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

> **Note:**
>
> Deleting an alarm in Oracle Communications Session Delivery Manager has no affect on the node because the node is unaware that Oracle Communications Session Delivery Manager 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 and click **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 Communications Session Delivery Manager.

1. Expand the **Fault Manager** slider and select from the following options:

   • **Events**

   • **Alarms**

2. In the events or alarms pane, click **Delete by criteria**.

3. In the **Delete event** 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.

Name	Description
Please specify the delete choice field	Click to select either **Delete all** or **Delete by criteria**.
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.
Device 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.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm or event.

4. Click **OK**.

Configure When Event and Alarm Data is Deleted

1. On the main menu, click **Settings** > **Faults** > **Fault configuration**.

2. In the **Fault configuration** dialog box, complete the following fields:

Name	Description
*Clear events older than (days) field	The number of days events are retained in the database before the events are cleared. The default value is seven days. Zero indicates no event data is cleared
*Clear alarms older than (days) field	The number of days alarms are retained in the database before the alarms are cleared. The default value is 14 days. Zero indicates no alarm data is cleared.
*Duplicate trap filter interval (minutes) field	The number of minutes for when duplicate traps are rejected for events and alarms.

3. Click **OK**.

4. In the success dialog box, 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 Communications Session Delivery Manager.

Configure the Auto Refresh Period for Alarm Data

> **Note:**
>
> Oracle recommends that the use of the auto refresh function is limited to two users or less, due to the functional expense of this operation.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. Click **Auto refresh**.
3. In the **Auto refresh** dialog box, enter the number of seconds to refresh alarm data in the **Refresh Interval(secs)** field.
4. Click **OK**.

> **Note:**
>
> If you want to stop the auto-refresh function, click **Stop Auto Refresh**.

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 and click **Edit**.
3. In the Edit annotation dialog box, add your explanatory note about this alarm in the **Annotation** field.
4. Click **OK**.

Enable Alarm Acknowledgement

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 Acknowledgement

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 Communications Session Delivery Manager has no affect on the node because the node is unaware that Oracle Communications Session Delivery Manager 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 and click **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 **Select** dialog box, select from the following alarm trap groups from the **Trap Groups** table:

   > **Note:**
   >
   > Oracle Communications Session Delivery Manager determines the trap groups that you can access.

   - **AcmeSD**—Session Delivery plugin trap group.
   - **SDM**—Default Oracle Communications Session Delivery Manager trap group.

3. In the **Trap Event Mapping Console** pane, select a trap from the **SNMP 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**.

Audible Alarms

The audible alarms system allows you to set off an audible sound when an activated alarm is triggered.

Alarm events are updated during each refresh cycle of the alarms table. Search functionality is disabled when audible alarms are active. The audible alarms cease to function upon exiting the Fault Manager navigation bar slider.

Audio Files

The Audible Alarms application comes with five alarm sounds (one for each severity). You may replace these files with your own files as long as the files retain the same filenames and are in a Waveform audio file format. The files are located in the following directory:

<installed directory>\ACMEConsole\audibleAlarms

The filenames appear as:

- Audio_Emergency.wav

- Audio_Critical.wav

- Audio_Major.wav

- Audio_Minor.wav

- Audio_Warning.wav

Enable and Configure Audible Alarms

1. On the main menu, click **Settings** > **Alarms** > **Audible Alarms**

2. In the **Audible Alarms** dialog box, click the check box next to the severity categories that you want to enable an audible alarm. The categories are **Emergency**, **Critical**, **Major**, **Minor**, and **Warning**.

3. Click **OK**.

4. On the Oracle Communications Session Delivery Manager navigation bar, select **Fault Manager** > **Alarms**

5. Click **Start Audible Alarm**.

   The button toggles to **Stop Audible Alarm**.

6. If you want to shut down the audible alarms application, click **Stop Audible Alarm**.

   The button toggles to **Start Audible Alarm**.

Change the Default Severity Alarm Colors

1. On the main menu, click **Settings** > **Alarms** > **Alarm Colors**

2. In the **Alarm colors** dialog box, click the **Color** drop-down list next to the severity category and its default color.

3. In the pop-up color palette, click the new color that you want for the alarm.

4. Repeat the previous two steps if you want to configure more severity alarm colors.

5. Click **OK**.

6. In the success **Information** dialog box, click **OK**.

Enable Alarm Synchronization

Use this task to retrieve alarms you may have missed from devices, if SDM was unavailable for a limited time period.

Pre-requisites:

*   You must have administrator privileges to do this task.

*   On the individual devices SDM manages that support alarm synchronization, you must specify how many days to keep traps by using the **trap-event-lifetime** parameter.

1. On the Oracle Communications Session Delivery Manager navigation bar, select **Device Manager** > **Devices**.

2. In the **Managed Devices - Group View** table tree, expand the tree and click the device for which you want to enable alarm synchronization.

3. Click **Admin** > **Synchronize alarms**.

4. In the **Synchronize alarms** dialog box, click **Yes**.

5. In the success dialog box, click **OK**.

6. Expand the **Security Manager** slider and select **Audit log** > **View** to verify if the alarms are synchronized.

Configure Fault Email Notifications

Oracle Communications Session Delivery Manager can trigger automatic email notifications when reporting alarms for certain severities. You can configure the appropriate email addresses that match each alarm severity.

> **Note:**
>
> You must configure the SDM mail server before you can use this feature. See the *Configure the Mail Server* section in the *Oracle Communications Session Delivery Manager Installation Guide* for more information.

Configure Email Notifications for Fault Occurrences

With appropriate administrator privileges assigned, you can assign fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.

2. In the **Fault email recipients** dialog box, click **Add**.

3. In the **Add email** dialog box, complete the following fields:

Name	Description
*Email address field	The recipient email address attached to the alarm severity.
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.

5. In the success dialog box, click **OK**.

6. In the **Fault email recipients** dialog box, the configured email address appears in the table. Click **OK**.

Delete Fault Email Notifications

With appropriate administrator privileges assigned, you can delete fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.

2. In the **Fault email recipients** dialog box, select the email address you want to remove and click **Delete**.

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

4. In the success dialog box, click **OK**.

5. In the **Fault email recipients** dialog box, the email address no longer appears in the table. Click **OK**

Edit Fault Email Notifications

With appropriate administrator privileges assigned, you can edit fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.

2. In the **Fault email recipients** dialog box, select the email address you want to edit and click **Edit**.

3. In the **Edit email** dialog box, edit the following fields:

Name	Description
*Email address field	The recipient email address attached to the alarm severity.

ORACLE®

Name	Description
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.

5. In the success dialog box, click **OK**.

6. In the **Fault email recipients** dialog box, the edited email address appears in the table. Click **OK**

View 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 SDM. When you select a trap group the product plugin, SNMP trap (OID) list is provided. 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. In the **Select** dialog box, select the **AcmeSD** trap group row from the **Trap groups** table and click **OK**.

3. The following table describes the Session Delivery product event types and a description that references its respective trap. If you need to customize the severity level of this trap, see the Customize Alarm Trap Severity Levels section for more information.

Session Delivery Manager Traps

The trap event setting allows you to override the core SDM 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 SDM product event types and a description that references its respective trap. If you need to customize the severity level of this trap, see the Customize Alarm Trap Severity Levels section for more information.

Trap	Description
apEMPluginDuplicatedRestPrefixName	The trap is generated when there is a plugin installation attempt that has the same name as an existing REST API prefix name in the system.
apEMPluginFailedInstall	The trap is generated whenever an element manager (EM) product plugin failed to install.
apEMPluginFailedInstallClear	The trap is generated whenever an EM product plugin failed installation status is recovered.
apEMPluginFailedUninstall	The trap is generated whenever an EM product plugin failed to uninstall.
apEMPluginFailedUninstallClear	The trap is generated whenever an EM product plugin failed to uninstall status is recovered.

ORACLE

Trap	Description
apEMSActivateFailure	The trap is generated when SDM fails to activate a configuration, whether initiated from the SOAP XML API or the SDM GUI for the save/activate or activate operations.
apEMSNodeUnreachable	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.
apEMSNodeUnreachableClear	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.
apEMSSaveFailure	The trap is generated when SDM fails to save a configuration. The trap is generated by a save failure whether initiated by the SOAP XML API or SDM GUI for the save/activate, save, or offline save operations. The trap contains the node ID of the device, the start and stop time of the save configuration attempt, and the user initiating the save operation.
apEMSDiscoveryFailure	The trap is generated whenever an error is detected during server node discovery.
apEMSInvalidConfigDiscovered	The trap is generated whenever an invalid configuration is retrieved from a node. Additional information about the validity failure is available in the discovery log.
apEMSInvalidConfigInventory	The trap is generated whenever an inventory check was performed and failed.
apNNCReportingHdrAggregationFailure	This trap is depricated. Use the apNNCReportingHdrAggregationLagFailure trap. This trap is generated when an SDM reporting HDR aggregation task fails to keep up with incoming HDR data.
apNNCReportingHdrAggregationLagFailure	The trap is generated when an SDM reporting HDR aggregation task fails to keep up with incoming HDR data.
apNNCReportingHdrAggregationLagFailureClear	The trap is generated when a previously failed SDM reporting HDR aggregation task is now able to stay current with incoming HDR data.
apNNCReportingHdrDetectionFailure	The trap is generated whenever an SDM reporting HDR detection task failed.
apNNCServerUnreachable	The trap is generated whenever an SDM server is determined to be unreachable by another an SDM server configured in the same cluster.
apNNCServerUnreachableClear	The trap is generated whenever a previously unreachable SDM server is determined to be reachable by another SDM server configured in the same cluster.

6
Manage Transport Layer Security Certificates

You can upload entity or trusted certificates to Oracle Communications Session Delivery Manager for east-west peer SDM server communication, and for southbound communication with network function (NF) devices.

> **Note:**
>
> This chapter does not discuss the importation or deletion of HTTPS Certificates for the web service. These actions are handled through the SDM setup installation program. Refer the *Configure Web Server Security* section in the *Oracle Communications Session Delivery Manager Installation Guide* for more information.

Trusted certificates use the X.509 cryptographic standard for security validation in a 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.

> **Note:**
>
> See the *Configure Transport Layer Security Certificates* section in the *Custom Installation* chapter of the *Oracle Communications Session Delivery Manager Installation Guide* for more information about generating and uploading an entity certificate for mutual authentication between a peer SDM server and southbound devices.

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) transport layer security (TLS) communication to applications, product plugins, and their respective NF devices that run on Oracle Communications Session Delivery Manager.

SDM communicates with devices indirectly through the installed *Oracle Communications Session Element Manager* product plug-in. For example, this plug-in may use ACP (plaintext or with TLS), SNMP, SSH, and SFTP to communicate with devices. TLS can be enabled for ACP to add security, but ACP itself provides no 'added security'. Refer to the specifications of your NF devices (client) to determine if an NF device supports the SBI TLS feature.

Upload a New Certificate

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

1. On the main menu, select **Tools** > **Certificates**.

2. In the **Certificates** dialog box, click **Import**.

3. In the **Upload Certificate** dialog box, complete the following fields:

Name	Description
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 SDM, you can delete an existing certificate from the SDM trust store.

1. On the main menu, select **Tools** > **Certificates**.

2. In the **Certificates** dialog box, click **Delete**.

3. In the **Delete** confirmation dialog box, click **Yes**.

7
Configure Northbound Interface Traps

You can specify northbound interface (destination) fault trap receivers for northbound systems, such as a network management system, to receive forwarded SNMP trap fault notifications in either SDM format or International Telecommunication Union (ITU) X.733 format. You can also configure the heartbeat trap for the northbound interface, which is discussed later in this chapter.

The SDM fault manager function forwards trap notifications over the northbound interface to the configured trap receiver system(s).

When you install a standalone SDM server or an SDM cluster, you must configure the global identifier (ID). When devices that are managed by SDM send SNMP traps, the global ID is embedded in the trap. When an administrator views the trap on their northbound system, the originating device can be determined by viewing global ID contained in the trap. See the *Specify the Global ID for Northbound Trap Receivers* section in the *Typical Installation* chapter of the *Oracle Communications Session Delivery Manager Installation Guide* for more information.

> **Note:**
>
> The global ID must be the same for all nodes in the same SDM cluster. If there is more than one cluster in a network, each cluster must use a different global ID.

In the following diagram, devices send all traps to the SDM server, which sorts them into events and alarms. Events are the aggregated list of all such messages while alarms record only the current state or latest event.

Figure 7-1   Device forwarding of SNMP trap fault notifications through SDM to a northbound trap receiver system
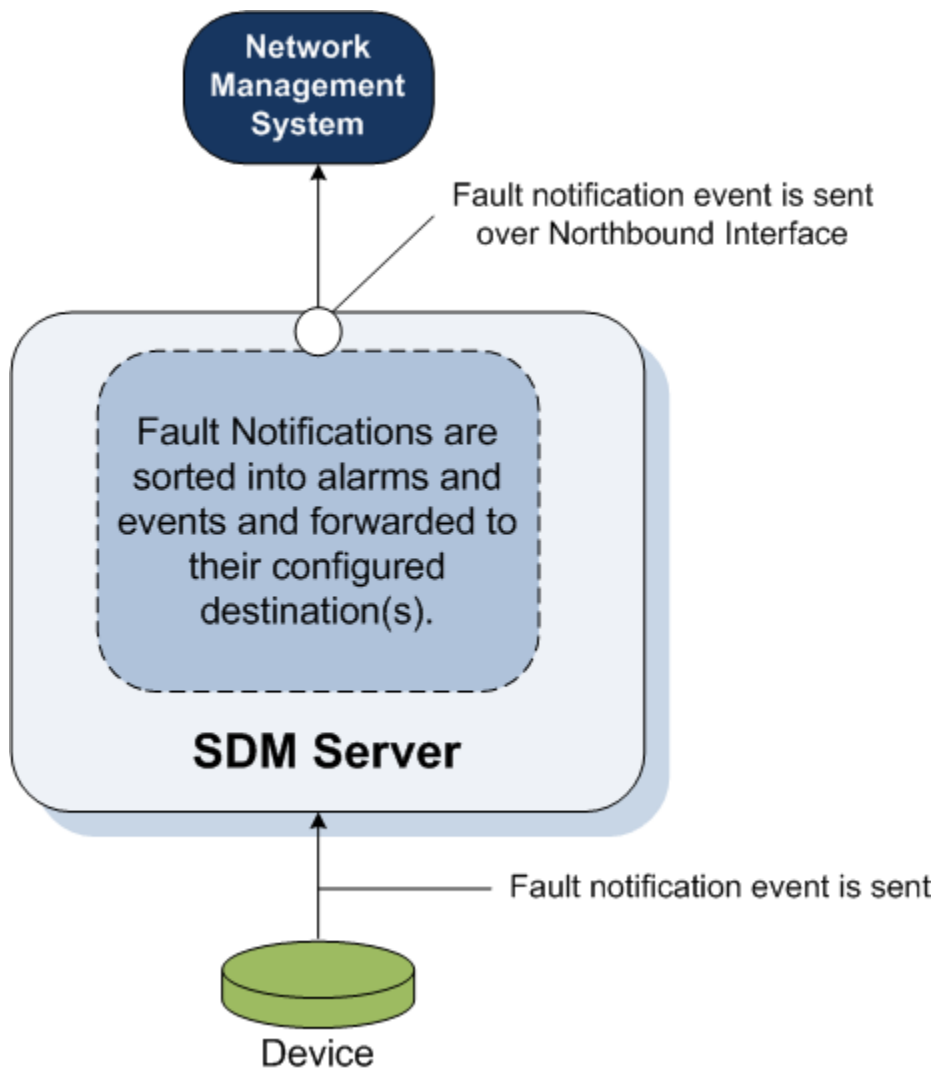
Configure Fault Notification on the Northbound Interface

Add a Northbound Fault Trap Receiver

Use this task to add a trap receiver, such as a network management system, that is connected to the northbound interface that receives fault notifications through the SDM server fault manager.

1. From the menu bar, select **Settings** > **Faults** > **Trap receivers** .

2. In the **Trap receivers configuration** table, click **Add**.

3. In the **Add trap receiver** dialog box, complete the following fields for the **Destination configuration**:

Name	Description
IP address	The IP address of the northbound trap receiver that is receiving traps.
UDP port	The trap receiver UDP port number. The default user datagram protocol (UDP) port is 162.
Community string	The SNMP community name to which the trap receiver belongs. The default value is **public**.
SNMP version drop-down list	The northbound trap receiver accepts SNMP version**V2** only.
Forward enabled check box	Check the check box to enable trap forwarding on this northbound trap receiver. Uncheck the check box to disable forwarding.

4. Complete the following fields for the **Filter configuration**:

Name	Description
Severity level drop-down list	Select a severity level from the following ITU X. 733 alarms: • **Indeterminate** (Unknown)—The trap severity cannot be determined because of the nature of the information contained in the trap. • **Critical** (Emergency)—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. • **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. • **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. • **Warning**—Warning conditions exist and there are some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. An alarm is forwarded if it is equal to the selected alarm or has a higher severity than the selected alarm.

Name	Description
Format field	Select from the following northbound trap formatting options: • Click the **OC SDM** radio button to forward traps from the SDM server to the northbound trap receiver in their originating format. • Click the **ITU X.733** radio button to convert traps from session delivery product devices to the northbound trap receiver in an International Telecommunication Union Alarm Model format defined in recommendation X.733 format.
OC SDM traps check box	Check the check box to enable all traps generated by the SDM server to be forwarded to this trap receiver.
Device traps check box	Check the check box to enable all traps generated by managed devices to be forwarded to this trap receiver.

5. Choose from the following options to specify the destination of traps:

   • Select the **All devices** radio button to send traps from all devices to all devices. If you select this option, you are finished.

   • Select the **Select devices** radio button to send traps from select devices to select devices. If you select this option, proceed to the next steps.

6. In the **Mangaged devices** table, expand the hierarchical group folder and navigate to the network function (NF) device you want as a trap source.

7. Select the device and click **Add**.

   The NF device appears in the **Selected trap source devices** table.

8. Repeat the previous two steps to add more devices.

> **Note:**
>
> A maximum of 10 trap receivers can be configured at once, regardless of the format.

9. Click **OK**.

   The trap receiver appears in the **Trap receivers configuration** table.

Manage Fault Notification on the Northbound Interface

Synchronize Alarms for a Northbound Fault Trap Receiver

A specified time period can be configured to synchronize northbound interface alarm fault trap notifications from devices that are managed by SDM to determine the health of devices.

When the alarm synchronization feature is configured for a specified time interval and enabled, traps are resent from devices to the northbound interface. The system administrator determines

which traps are new and which are duplicates. A system administrator uses this feature to ensure that device alarm fault trap notifications received on their northbound systems are current with the alarm trap notification generated by the device or in situations when previous traps are lost on SDM or the northbound system and need to be regained from the device.

> **Note:**
>
> The **Start time** fields default to 24 hours prior to the current time and the **End time** fields default to the current time.

1. From the menu bar, select **Settings** > **Faults** > **Trap receivers** .

2. In the **Trap receivers configuration** table, select a trap receiver and click **Sync**.

3. In the **Trap receiver alarm synchronization** dialog box, complete the following fields:

Name	Description
Synchronization from	Select from the following options: • Click the **Event** radio button to synchronize the aggregated list of all trap messages. • Click the **Alarm** radio button to select the current device state or latest event trap messages.
Minimum severity level	Select from the following ITU X.733 alarm severity levels: • **Indeterminate** (Unknown)—Clear all events and synchronize from when they were cleared. • **Critical** (Emergency)—Send critical events or alarms. • **Major**—Send major and critical events or alarms. • **Minor**—Send minor, major, and critical events or alarms. • **Warning**—Send warning, minor, major, and critical events or alarms.
Start time field	To specify the start date, enter the month, day, and year (mm/dd/yyyy) or click the calendar icon to select the date and enter the time in the hour, minute, and second format (hh:mm:ss).
End time field	To specify the end date, enter the month, day, and year (mm/dd/yyyy) or click the calendar icon to select the date and enter the time in the hour, minute, and second format (hh:mm:ss).

4. Click **OK**.

5. In the confirmation dialog box, a message displays indicating the total number of events or alarms to be synchronized based on the parameters that you configured in this task. Click **Yes** to synchronize them.

Edit a Northbound Fault Trap Receiver

1. From the menu bar, select **Settings** > **Faults** > **Trap receivers** .

2. In the **Trap receivers configuration** table, click **Edit**.

3. In the **Edit trap receiver** dialog box, you can edit the following fields for the **Destination configuration**:

Name	Description
IP address	The IP address of the northbound trap receiver.
UDP port	The default user datagram protocol (UDP) port is 162.
Community string	The SNMP community name.
SNMP version drop-down list	The northbound trap receiver accepts SNMP version **V2** only.
Forward enabled check box	Check the check box to enable trap forwarding on this northbound trap receiver. Uncheck the check box to disable forwarding.

4. Edit the following fields for the **Filter configuration**:

Name	Description
Severity level drop-down list	Select from the following ITU X.733 alarms: • **Indeterminate** (Unknown). • **Critical** (Emergency)—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. • **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. • **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. • **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. An alarm is forwarded if it is equal to the selected alarm or has a higher severity than the selected alarm.

Name	Description
Format field	Select from the following northbound trap formatting options: • Click the **OC SDM** radio button to forward traps from the SDM server to the northbound trap receiver in their originating format. • Click the **ITU X.733** radio button to convert traps from session delivery product devices to the northbound trap receiver in an ITU X. 733 format.
OC SDM traps check box	Check the check box to enable all traps generated by the SDM server to be forwarded to this trap receiver.
Device traps check box	Check the check box to enable all traps generated by managed devices to be forwarded to this trap receiver.

5. You can edit the following options to specify the destination of traps:

   • Select the **All devices** radio button to send traps to all devices. If you select this option, you are finished.

   • Select the **Select devices** radio button to send traps to select devices. If you select this option, proceed to the next steps.

6. If you need to add a device to the **Mangaged devices** table, expand the hierarchical group folder and navigate to the network function (NF) device you want as a trap source.

7. Select the device and click **Add**.

   The NF device appears in the **Selected trap source devices** table.

8. Repeat the previous two steps to add more devices.

> **Note:**
>
> A maximum of 10 trap receivers can be configured at once, regardless of the format.

9. If you need to remove a device to the **Selected trap source devices** table, expand the hierarchical group folder and navigate to the network function (NF) device you want as a trap source.

10. Select the device and click **Remove**.

    The NF device appears in the **Mangaged devices** table.

11. Repeat the previous two steps to remove more devices.

12. Click **OK**.

    The trap receiver appears in the **Trap receivers configuration** table.

View Northbound Fault Trap Receivers

1. From the menu bar, select **Settings** > **Faults** > **Trap receivers**.

2. In the **Trap receivers configuration** table, view the following trap receiver column information:

Name	Description
IP address	The northbound trap receiver IP address.
UDP port	The default user datagram protocol (UDP) port is 162. UDP is used for establishing low-latency and loss tolerating connections. Change the default UDP port if you are using a different port for UDP connections.
SNMP version	The trap receiver SNMP version, which can be version 2 (V2) only.
Community string	The SNMP community name.
Forward enabled	Indicates whether the trap receiver is enabled (**True**) or disabled (**False**).
Status	The following trap receiver status conditions are possible: • **Enabled** • **Disabled** • **Suspended** • **Syncing** • **SyncSucceed** • **SyncFailed**
Format	(Hidden) Indicates if a trap receiver is either in NNC (SDM server) format, or ITU for ITU X. 733 format. If the trap receiver uses the ITU X. 733 format, the SDM fault manager converts traps from its host(s) to the ITU X.733 format.
Severity	(Hidden) The alarms that have a severity level that affects service are forwarded.
Object ID	(Hidden) The internal SDM element object ID number.

The following example shows all available columns for three configured northbound trap receivers (network management systems).

Figure 7-2   Trap Receivers Configuration table

Delete a Northbound Fault Trap Receiver

1. From the menu bar, select **Settings** > **Faults** > **Trap receivers**.

2. In the **Trap receivers configuration** table, select a network function (NF) device trap receiver and click **Delete**.

3. In the **Success** dialog box, click **OK**.

Configure Heartbeat Notification on the Northbound Interface

The heartbeat trap (apOCSDMServerHeartbeatReachable) can be manually started and stopped to periodically monitor the availability of the SDM from the northbound interface. This heartbeat trap is sent (forwarded) out of the northbound interface as an event (INFO) to the connected destination trap receiver of a management device. A problem can be detected by the management device if no heartbeat trap is received by its trap receiver during the specified interval due to either the failure of a standalone SDM server or SDM cluster, or if SNMP administrative changes affected the connectivity between the SDM server and the northbound system.

> **Note:**
>
> You must add a northbound interface (external) SNMP trap receiver to SDM before doing this task. See the Configure Northbound Interface Fault Trap Receivers section for more information.

The heartbeat trap is disabled by default and this task is optional. Use the following steps to specify the heartbeat trap send interval, and initiate the sending or termination of a heartbeat trap to a a northbound interface (external) SNMP trap receiver.

1. From the menu bar, select **Settings** > **Faults** > **Heartbeat Traps**.

2. In the **Configure heartbeat SNMP trap interval** dialog box, complete the following fields:

Name	Description
Interval (minutes) drop-down list	Select the number of minutes to send the heartbeat trap. The range increments in 5 (default), 10, 15, 30 and 60 minutes.
Start field	(Read-only) The time the last heartbeat trap was started.
Stop field	(Read-only) The time the last heartbeat trap was stopped.
Trap time stamp field	(Read-only) The time stamp for when the last heartbeat trap was sent.

3. Click **Apply** to update the interval change.

4. Click **Start** to send the heartbeat trap. The heartbeat trap is sent at the interval that you specify.

> **Note:**
>
> You can click **Refresh** to see the most current trap time stamp information for exactly when the last heartbeat trap was sent. You can also click **Stop** at any time if you need to stop the heartbeat trap.

8

Monitor Session Delivery Manager Server Health and Disk Usage

Use the **Health Monitor Console** pane to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics.

Use the Health Monitor to Determine SDM Server Health

A heartbeat is a server message that essentially says that it is active. The Health Monitor maintains SDM server statistics and heartbeats for all SDM cluster nodes. It also keeps a count of the times a node was considered inactive and the number of times the node returned to an active state based on the number of received and missed heartbeats.

1. From the menu bar, select **Tools** > **Health Monitor**.

2. In the **Health Monitor Console** display, select **Heartbeat** from the **Select Monitor** drop-down list.

3. The default IP address for this node is displayed in the **Select Source** drop-down list. If this node is part of a cluster, you can check the health status for another node by selecting its IP address from the **Select Source** drop-down list. The following table columns are described below for the targeted node:

Name	Description
Cluster Member	The IP address of the cluster node. If the IP address of the node has the (Master) label appended, this node is running the master replication database.
Status	The following status applies for a cluster node: • **ACTIVE**—This node is actively participating in the cluster. • **DOWN**—The node failed to send its heartbeats, is in a failed state, or a network partition exists between the cluster and this node.
Up Time (dd:hh:mm)	The number of days, hours, and minutes the node has been active.
Down Time (dd:hh:mm)	The number of days, hours, and minutes the node has been down.
Last Heartbeat Timestamp	The date and time of the last known heartbeat of the node.
Heartbeat Count	The total number of node heartbeats.

Name	Description
Missed Heartbeat Count	The total number of times the heartbeat monitor on this node missed a heartbeat from other nodes in the cluster.

> ✎ **Note:**
>
> An increase in this statistic might indicate network issues between nodes in the cluster.

Name	Description
HBFM	The Heartbeat Failure Meter (HBFM) statistic indicates the amount of times the required heartbeat counter of a node was not received. This number increases when the heartbeats start arriving again. If this statistic reaches a count of 10 (default) the node status is **DOWN**.
MHFM	The Maximum Heartbeat Failed Meter (MHFM) statistic maintains the high-water mark of the HBFM statistic. This statistic is only reset if a node that left the cluster (status=**DOWN**) rejoins and starts sending heartbeats again.
Inactivity Count	The number of times the node was considered to be in the **DOWN** state.
Reset Count	Number of times the node has gone from a state of **DOWN** to a state of **ACTIVE**. If the node rejoins the cluster after being **DOWN**, the reset counter is incremented by 1 and the MHFM is reset to 0.

Monitor SDM Server Disk Usage

Use the **Disk Usage** monitor on a selected SDM server node to check if disk usage exceeds the 50 and 90 percent thresholds and inspect disk storage usage by gathering statistics for total disk storage, used disk capacity, and free disk capacity. You can also display the SDM server directory size and view the partition on which the directory is located. For example, a database directory might be located on a different partition from other directories.

View Summary SDM Server Disk Usage Statistics

1. From the menu bar, select **Tools** > **Health Monitor**.

2. In the **Health Monitor Console** pane, select **Disk Usage** from the **Select Monitor** drop-down list.

3. Select the SDM server node IP address from the **Select Source** drop-down list (if the node is a member of a cluster) or retain the default value if the node is a standalone node. In the **Summary** tab, the following table describes the storage statistics fields:

Name	Description
Cluster member	The node name.
Path	The directory path where the node is installed.

Name	Description
Status	The following status partition space status conditions can occur: • **Normal**—The partition space is below the minimum threshold value, which is fifty percent (default). • **Warning**—The partition space is at or above the minimum threshold value of fifty percent (default), but below the maximum threshold value of ninety percent (default). • **Critical**—The partition space is at or above the maximum threshold value of ninety percent (default).
Capacity	The total partition disk space in gigabytes (GB).
System Used Space	Total amount of disk space being used.
Free Space	The remaining disk space in GB.
Percent Usage	The percent of used disk space for the entire partition.

View Detailed SDM Server Disk Usage Statistics

1. From the menu bar, select **Tools** > **Health Monitor**.

2. In the **Health Monitor Console** pane, select **Disk Usage** from the **Select Monitor** drop-down list.

3. Select the SDM node IP address from the **Select Source** drop-down list (if the node is a member of a cluster) or retain the default value if the node is a standalone node. In the **Details** tab, the following table describes the director storage statistics fields:

Name	Description
Partition	The name of the partition where the directory is located.
Path	The directory path where the SDM server software, RMCArchive, or SDM database is installed.
Directory Size	The amount of disk space used in the directory in gigabytes (GB).
Percent Usage	The percentage of partition space being used by the specific directory.

9

Session Delivery Manager Server Database Maintenance

Use this chapter to perform maintenance on standalone or cluster SDM servers, which includes backing up and restoring the SDM application database and Oracle reporting databases and cluster management.

Backup or Restore Databases

Use the tasks in this section to backup or restore the SDM server application and reporting databases.

Backup Command Options

Use the following command line options when issuing the backup script in the following sections to specify your database and backup destination:

--all —(Default) Backs up the core database and all reporting databases. This flag is used if no other is entered.

--core —Backs up the core database only.

-d —Specifies the directory to store the backed up file.

--excludePlugins —Exclude archived Plugin zip files from the resulting backup file. By default, the resulting backup file contains all product plugin installation zip files which were previously uploaded to SDM. You can override this behavior by entering this command.

-ep —Same as the --excludePlugins command line option above.

--report —Backs up the reporting oracle database and repository.

--ocsdmdw —Backs up the ocsdmdw oracle database.

> **Note:**
>
> You are prompted to select the backup directory upon running a backup script. The default directory can be found at: `<Installation directory>/../DatabaseBackup`

Backup Databases on a Shutdown Server

The following sections describe how to backup the application database on an SDM server that is shutdown (cold backup).

> **Note:**
>
> You must have system administrator privileges on the server to do a database backup.

The SDM database and a separate database for reporting (if you are using Oracle Communications Report Manager with SDM) runs on each cluster node. During a typical database backup, the backup for each of these database is done on the master node and the backup file is stored on the node running the backup only.

Shut Down the System

You can shut down the existing SDM software version running on your system to install a new version of the software, restore a database or apply a software patch.

1. Log in as the nncentral user.

2. Change directory to the bin directory.

   For example:

   ```
   cd /home/nncentral/AcmePacket/NNC<version>/bin
   ```

3. Execute the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

   > **Note:**
   >
   > However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

   ```
   ./shutdownnnc.sh
   Shutdown back-end server
   Do you wish to shut down the entire cluster (Yes/No)? Yes
   ```

Backup the Database on the Shutdown Server

Use this task to do a backup the application database (Core DB), Oracle reporting database, and OCSDMDW reporting database on the shut down SDM server (cold backup) to a local directory path.

1. If you are using Oracle Communications Report Manager, you must shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW) before you do the cold backup of the database. See the Report Manager Administrator Operations chapter in the *Oracle Communications Report Manager Installation Guide* for more information about stopping these database instances.

2. Login to the server as the nncentral user.

3. Change to the bin directory. For example:

   ```
   cd /home/nncentral/AcmePacket/NNC8x/bin/
   ```

4. Enter the **backupdbcold.sh** script.

> **✏ Note:**
>
> The **backupdbcold.sh -- help** script provides all of the arguments that you can use.

```
./backupdbcold.sh
```

- You can use the following arguments with this script:

  - **-d** —Use this argument to select a local directory that you want to store backup archives. For example:

    ```
    ./backupdbcold.sh -d/home/nncentral/AcmePacket/<Directory>/
    NNC8x_ColdBackup_yyyy_mm_dd_<number>_all.tar
    ```

  - **-a**, **--all** — Use this argument to run all backups and store them as a single archive.

    ```
    ./backupdbcold.sh --all
    ```

  - **-c --core** — Use this argument to backup the core application database and store it as an individual archive.

    ```
    ./backupdbcold.sh --core
    ```

  - **-r --report** — Use this argument to backup the reporting Oracle database and repository and store as an individual archive.

    ```
    ./backupdbcold.sh --report
    ```

  - **-o --ocsdmdw** — Use this argument to backup the (Oracle Communications Session Delivery Manager Data Warehouse (OCSDMDW) database and store as an individual archive.

    ```
    ./backupdbcold.sh --ocsdmdw
    ```

  - **-ep**, **--excludePlugins** —Use this argument to exclude archived plugin zip files from the resulting backup file. By default, the resulting backup file contains all product plugin installation zip files which were previously uploaded to SDM. You can override this behavior by entering this command.

    ```
    ./backupdbcold.sh --excludePlugins
    ```

After the script runs, the output displays a section called **Backup Results**. The output shows if the core SDM application database and reporting databases are successfully backed up to the default **DatabaseBackup** directory. The following example shows the directory on which the application database file was backed up:

```
/home/nncentral/AcmePacket/DatabaseBackup/
NNC8x_ColdBackup_yyyy_mm_dd_<number>_all.tar
```

> **✏ Note:**
>
> If you do not have reporting configured on the SDM server, the output shows that the reporting databases failed to be backed up.

5. Execute the **startnnc.sh** script.

> **Note:**
>
> With the introduction of Oracle Communications Session Delivery Manager,
> Release 8.0, you must select one server to start in the cluster only. Once this server
> is started and operational, you can start the other server(s) in the cluster.

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the
system is ready for use. Do not attempt to log in until the console has indicated that the
web servers are up.

6. If you are using Oracle Communications Report Manager and have shut down the Oracle
   BI Publisher database instance and Oracle Report Manager database instance
   (OCSDMDW), you must start them again. See the Report Manager Administrator
   Operations chapter in the *Oracle Communications Report Manager Installation Guide* for
   more information about starting these database instances.

   The SDM plugin service always tries to synchronize itself with other cluster nodes when
   the server starts. This allows a node that was previously down, become current if it missed
   an upload, or an uninstall event.

Next Steps

- Select **Tools** > **Health Monitor** and view the **Heartbeat Summary** table to check SDM
  cluster member node processes.

- Begin using SDM. Use your web browser to navigate to the server login page by entering
  the host name or IP address, and port number in the web browser navigation bar. For
  example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in
the *Configure User Account Passwords* section.

Backup Databases on a Running Server

Use this task to do a backup the application database (Core DB), Oracle reporting database, and
OCSDMDW reporting database on the SDM server that is running (hot backup) to a local
directory path.

> **Note:**
>
> Before you backup databases on the SDM server, ensure that you have system
> administrator privileges, and contact users to minimize or prevent them from using
> SDM during the backup.

1. Login to the server as the nncentral user.

2. Change to the bin directory. For example:

```
cd /home/nncentral/AcmePacket/NNC8x/bin/
```

3. Enter the **backupdbhot.sh** script to backup the application and reporting databases.

> **Note:**
>
> The **backupdbhot.sh -- help** script provides all of the arguments that you can use.

```
./backupdbhot.sh
```

- You can use the following arguments with this script:
  - **-d** —Use this argument to select a local directory that you want to store backup archives. For example:

    ```
    ./backupdbhot.sh -d/home/nncentral/AcmePacket/<Directory>/
    NNC8x_HotBackup_yyyy_mm_dd_<number>_all.tar
    ```

  - **-a**, **--all** — Use this argument to run all backups and store them as a single archive.

    ```
    ./backupdbhot.sh --all
    ```

  - **-c --core** — Use this argument to backup the core application database and store it as an individual archive.

    ```
    ./backupdbhot.sh --core
    ```

  - **-r --report** — Use this argument to backup the reporting Oracle database and repository and store as an individual archive.

    ```
    ./backupdbhot.sh --report
    ```

  - **-o --ocsdmdw** — Use this argument to backup the (Oracle Communications Session Delivery Manager Data Warehouse (OCSDMDW) database and store as an individual archive.

    ```
    ./backupdbhot.sh --ocsdmdw
    ```

  - **-ep**, **--excludePlugins** —Use this argument to exclude archived plugin zip files from the resulting backup file. By default, the resulting backup file contains all product plugin installation zip files which were previously uploaded to SDM. You can override this behavior by entering this command.

    ```
    ./backupdbhot.sh --excludePlugins
    ```

After the script runs, the output displays a section called **Backup Results**. The output shows if the core SDM application database and reporting databases are successfully backed up to the default **DatabaseBackup** directory. The SDM plugin service always tries to synchronize itself with other cluster nodes when the server starts. This allows a node that was previously down, become current if it missed an upload, or an uninstall event.The following example shows the directory on which the application database file was backed up:

```
/home/nncentral/AcmePacket/DatabaseBackup/
NNC8x_HotBackup_yyyy_mm_dd_<number>_all.tar
```

> **Note:**
>
> If you do not have reporting configured on the SDM server, the output shows that the reporting databases failed to be backed up.

Next Steps

- Select **Tools** > **Health Monitor** and view the **Heartbeat Summary** table to check SDM cluster member node processes.

- Begin using SDM. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

Restore Databases

Use this task if you need to restore the application and reporting databases on your SDM system or cluster.

1. Login to the server as the nncentral user.

2. Change to the bin directory. For example:

```
cd /home/nncentral/AcmePacket/NNC8x/bin
```

3. Execute the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

> **Note:**
>
> However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

```
./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
```

4. If you want to perform a backup of the application or reporting databases on the running SDM server (hot backup), see the Backup the Database on a Running Server section for more information, and skip to step 5.

5. If you want to perform a backup of the application or reporting databases on a shut down server (cold backup) see the Backup the Database on a Shutdown Server for more information, and skip to step 5.

6. If you need to restore the application database only (you are not using the reporting databases) on your SDM system, enter the **restoredb.sh** script followed by the directory in which the backup application database is stored. For example:

```
./restoredb.sh -f/home/nncentral/AcmePacket/NNC8x/bin/
NNC8x_Backup_2017_04_19.tar.gz
```

If you need to restore the application database and the reporting databases on your SDM system, enter the **restoredb.sh** script followed by the directory in which the backup application database is stored, and specify the Oracle reporting database password and OCSDMDW reporting database password:

```
./restoredb.sh -f/home/nncentral/AcmePacket/NNC8x/bin/
NNC8x_Backup_2017_04_19.tar.gz -z my_report_db_password -y
my_ocsdmdw_db_password
```

ORACLE

7. If you are using Oracle Communications Report Manager and have shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW), you must restart them. See the *Report Manager Administrator Operations* chapter in the *Oracle Communications Report Manager Installation Guide* for more information about starting these database instances.

8. Execute the **startnnc.sh** script. For example:

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up.

Next Steps

- Select **Tools** > **Health Monitor** and view the **Heartbeat Summary** table to check SDM cluster member node processes.

- Begin using SDM. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

- After the server starts (after the restoration of its databases), it attempts to synchronize all plugins installed on the local file system again. Select **Tools** > **Plugin Management** in the SDM GUI to ensure that all plugins are working properly in the **Element Manager Plugins** table.

10
Session Delivery Manager Server Cluster Maintenance

Use this chapter to perform cluster maintenance on SDM servers, which includes information about how the automatic cluster recovery process works and the different methods that can be employed to maintain SDM cluster operation.

A cluster can operate as a two-node or multi-node cluster. The master node contains the database for configuration data and no replication of large configurations is required. The failure of a node does not effect on-demand retrieval of configuration from devices serviced by other nodes.

A two-node cluster has one master node and one replica node. The following recovery scenarios can occur when one node fails:

- If the master node fails in a two-node cluster, the remaining replica node becomes master. The non-operational tries to recover and rejoin the cluster. If the node is non-operational for more than 24 hours, the cluster needs to be manually restored.

- If network connectivity is lost between the two active nodes in a two-node cluster, a network partition occurs that causes both members to become masters. Once network connectivity is re-established and the network partition is resolved, the Berkley database elects one node master and the other node shuts down and restarts as the replica node.

A multi-node cluster has one master node that has multiple replicas. If a master database failure occurs in a cluster with multiple replicas, re-election among the replicated database occurs and a new master database is elected. Transactions are successful on a three or more node cluster if a quorum of replies from replicas is achieved only to guarantee that the data exists on more than the master database after the transaction completes. If a quorum is not met, then the transaction fails.

Message events and data is distributed in the cluster through the MOM, which is based on a store and forward process and guarantees message delivery by storing the message in a local database first before declaring that the message was properly processed. In a MOM cluster, there is no master node because all MOM brokers that participate in the cluster ensure that messages are synchronized in the cluster. Durable subscribers ensure that even if a node leaves the cluster and reenters within a 24 hour period, missed messages are re-delivered. Tasks entered in a queue are processed even if the host where the task was originally submitted goes down.

Automatic Cluster Recovery Process

An automatic synchronization of nodes can occur when there is a temporary communication outage between cluster nodes (possibly due to network issues). During this time, each node can temporarily leave the cluster and automatically rejoin the cluster and synchronize data with the XML databases of the local master cluster node and replication group.

The following automatic recovery processes deploy when a node fails or is shutdown:

- The Berkley XML database insures that remaining replicas carry out an election and elect a new master, when the member that leaves is running the master database.

- The Message-Oriented Middleware (MOM) service maintains topic messages for any durable subscribers registered on the host that departed. These messages are maintained for 24 hours before they are removed.

- Any services that share common task processing on the node that departed the cluster. Submitted tasks, such as save and activate or the poller are processed by the remaining cluster members.

- Any services acquiring a lock, such as device synchronization, are removed after an expiration time on a node that departed the cluster. If the original service cannot remove the lock, it automatically expires.

- Any tasks initiated by a node that departed the cluster is re-submitted.

- Load balancers on the active nodes in the cluster bypass the front end node that left the cluster. Clients are redirected to a valid running node.

- The health monitoring service determines if the heartbeat of a node failed and publishes a failed message to all active cluster nodes that a node has left the cluster.

- The node attempts to synchronize its plugins to match the collective status of the cluster. This process might result in the retrieval of plugin zip files from other cluster nodes which were uploaded while the node was down and the installation, uninstallation, or deletion of a plugin while the node was down.

Remove a Cluster Node

> **Note:**
>
> Oracle recommends that you perform this task during a planned downtime, such as a maintenance period to avoid system disruption.

1. Log into the SDM GUI on a node belonging to the running cluster.

2. Select **Tools** > **Health Monitor**.

3. In the **Health Monitor Console** pane, view the **Heartbeat Summary** table to know which node is cluster member node that is running the master databases.

4. Log into the node to be removed from the cluster as the nncentral user.

5. Change directory to the bin directory.

   For example:

   ```
   cd /home/nncentral/AcmePacket/NNC8x/bin
   ```

6. Execute the **shutdownnnc.sh** script.

   ```
   ./shutdownnnc.sh
   ```

7. Uninstall SDM.

   ```
   ./uninstall.sh
   ```

8. Shut down all remaining nodes starting with the replicas, followed by the master cluster member node.

   ```
   ./shutdownnnc.sh
   ```

9. Switch to the root user on the master cluster member node and enter the root user password when you are prompted.

    `su root`

10. From the bin directory on the master cluster member node, execute the **setup.sh** script.

    `./setup.sh`

11. Enter **2** for the **Custom** option and press Enter.

12. Enter **Yes** to continue.

13. Enter **6** for the **Cluster management** option and press Enter.

14. Enter **Yes** to continue.

15. Option **1 Configure and manage members in a cluster** is selected by default. Press Enter.

16. Enter **Yes** to continue.

17. Enter **2** for the `Remove all remote members` option that removes all remote cluster member nodes from the cluster configuration and press Enter.

18. Enter **Yes** to continue.

19. Enter **1** for the **Proceed with removing all remote members** option and press Enter.

20. Enter **Yes** to continue.

21. Enter **3** for the **Apply new cluster configuration** option and press Enter.

22. Enter **Yes** to continue.

23. Enter **3** for the **Quit out of cluster configuration** option and press Enter.

24. Switch to the nncentral user on the master cluster member node.

    `su nncentral`

25. Execute the **startnnc.sh** script on the master cluster member node.

    `./startnnc.sh`

26. Execute the **startnnc.sh** script on each remaining replica node in the cluster.

Rejoin a Cluster Node Manually

Use this task to rejoin a cluster node manually with the cluster when this node is down for more than 24 hours, has a failure, or it is stopped.

> **Note:**
>
> Oracle recommends that you perform this task during a planned downtime, such as a maintenance period to avoid system disruption.

1. Log into the SDM GUI on a node belonging to the running cluster.

2. Select **Tools** > **Health Monitor**.

3. In the **Health Monitor Console** pane, view the **Heartbeat Summary** table and record the cluster member node that is running the master databases.

4. Log into the master cluster member node as the nncentral user.

5. Change directory to the bin directory.

For example:

```
cd /home/nncentral/AcmePacket/NNC8x/bin
```

6. Execute the **shutdownnnc.sh** script on the master cluster member node. By default, the shutdownnnc.sh script detects the clustered system and enter **Yes** when prompted to shut down the entire cluster.

```
./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
```

7. Enter the **backupdbcold.sh** script on the master cluster member node.

```
./backupdbcold.sh
```

8. Restore the databases on the master cluster member node If you need to restore the application database and the reporting databases on your SDM system, enter the **restoredb.sh** script followed by the directory in which the backup application database is stored, and specify the Oracle reporting database password and OCSDMDW reporting database password:

```
./restoredb.sh -f/home/nncentral/AcmePacket/NNC8x/bin/
NNC8x_Backup_2017_04_19.tar.gz -z my_report_db_password -y
my_ocsdmdw_db_password
```

9. If you are using Oracle Communications Report Manager and have shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW), you must restart them. See the *Report Manager Administrator Operations* chapter in the *Oracle Communications Report Manager Installation Guide* for more information about starting these database instances.

10. Execute the **startnnc.sh** script on the cluster member node that is down that needs to rejoin the cluster.

```
./startnnc.sh
```

11. Execute the **startnnc.sh** script on the master cluster member node.

```
./startnnc.sh
```

Next Steps

- Select **Tools** > **Health Monitor** and view the **Heartbeat Summary** table to check SDM cluster member node processes.

- Begin using SDM. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

- After the server starts after the backup of its databases, it attempts to synchronize all plugins installed on the local file system again. Select **Tools** > **Plugin Management** in the SDM GUI to ensure that all plugins are working properly in the **Element Manager Plugins** table.

Restore a Two Node Cluster

If one node in a two-node SDM cluster becomes non-operational, the non-operational node tries to recover and rejoin the cluster. However, if this node is non-operational for more than 24 hours, use this task to restore the two-node cluster.

> **Note:**
>
> With the introduction of Oracle Communications Session Delivery Manager, Release 8.0, you must select one server to start in the cluster only. Once this server is started and operational, you can start the other server(s) in the cluster. When connectivity between nodes is re-established automatically or manually, the Berkley XML database decides which node becomes the master.

1. Login to the operational node as the nncentral user.

2. Change to the bin directory on the operational node. For example:

   ```
   cd /home/nncentral/AcmePacket/NNC8x/bin/
   ```

3. Enter the **backupdbhot.sh** script to do a hot backup of the application and reporting databases on the operational node.

   ```
   ./backupdbhot.sh
   ```

4. On the shut down node, login as the nncentral user, navigate to the bin directory, and enter the **reinitialize.sh** script.

   ```
   ./reinitialize.sh
   ```

5. Go back to the operational node, and restore the application database and the reporting databases on your SDM two-node cluster, enter the **restoredb.sh** script followed by the directory in which the backup application database is stored. If applicable, you can also specify the Oracle reporting database password and OCSDMDW reporting database password. For example:

   ```
   ./restoredb.sh -f/home/nncentral/AcmePacket/NNC8x/bin/
   NNC8x_Backup_2017_04_19.tar.gz -z my_report_db_password -y
   my_ocsdmdw_db_password
   ```

6. On the shut down node, enter the **startnnc.sh** script. For example:

   ```
   ./startnnc.sh
   ```

Multiple Node Cluster Restoration

A partition results when network connectivity is lost between multiple SDM nodes in a cluster.

Typically, a multiple-node cluster consists of three nodes. When network connectivity is lost in this scenario, the partition that has two nodes and can communicate, elects a master. The partition that contains the single, orphaned node transitions to a READ-ONLY mode.

When network connectivity is re-established for the multiple-node cluster, one node is elected master and the cluster resumes normal operation. Database updates are not permitted until the partition between all nodes of the cluster is resolved or the cluster is reconfigured.

Configure a Clustered Server to be a Standalone Server

You can configure a clustered server to be a standalone server by removing its cluster configuration.

1. From the cluster management menu, select option 2, **Run current host as a standalone**. Press Enter to continue.

2. Select option 1, **Configure application server to a standalone server**. Press Enter to continue.

3. Select option 3, **Quit out of cluster configuration**.

4. Select option 2, **No**.

A

Available Session Delivery Manager Server Scripts

The following SDM server scripts are available for use by system administrators.

> **Note:**
>
> Contact your Oracle support representative before running any scripts that are not included in the list below. Running scripts not included in the list below may affect the functionality of your deployment.

Script Location	Description
./bin/setup.sh	The script launches the SDM installation tool.
./bin/uninstall.sh	The script launches the SDM uninstall tool.
./bin/startnnc.sh	The script starts the SDM server.
./bin/shutdownnnc.sh	The script shuts down the SDM server.
./bin/showallprocesses.sh	The script show all running processes on the SDM server.
./bin/collectinfo.sh	The script collects logs and system settings for the SDM server and optionally for any database backups that occur.
./bin/reinitialize.sh	The script reinitializes the database and permanently clears the data it contains.
./bin/reinitialize_ocsdmdw.sh	The script reinitializes the Oracle database instance for Oracle Communications Report Manager (OCSDMDW).
./bin/backupdbcold.sh	The script backs up the database on the SDM server when it is shutdown.
./bin/backupdbhot.sh	The script backs up the database on a running SDM server.
./bin/restoredb.sh	The script restores the database on the SDM server when it is shutdown.
./bin/backup_bip.sh	The script backs up the Oracle Business Intelligence (BI) Publisher database.
./bin/restore_bip.sh	The script restores the Oracle Business Intelligence (BI) Publisher database.

B

Fault Trap Notification Contents

A northbound interface fault trap contains specific information about the device from which it originates and SDM, which manages this device.

The SDM fault manager forwards an SNMP trap fault notification that is originated from the managed object instance (device or device object) that it manages to a network management system (such as an SNMP manager) through its northbound interface. The northbound network management system uses the SNMP trap fault notification sent by the managed object instance to identify specifically where the originator of the SNMP trap fault notification comes from. Network administrators use the information contained in the trap received by the northbound system to identify the origin of faults because this northbound system receives traps from many sources over the entirety of its network so that any problems can be addressed quickly and efficiently as they occur.

The following table describes the way information is formatted in the SNMP trap fault notification originating from a specific device that a specific SDM standalone server or server cluster manages:

Table B-1   Format of an SNMP trap fault notification from a managed object

Managed Object Instance::=<MO_Name>.<SDMGlobalName>;<IP_address>;<MO_Detail>
MO_Name::=<ManagedObjectClassName>
SDMGlobalName::=<SDMGlobalNameString>
IP_address::= The trap originator's IP address
MO_Detail::=<ManagedObjectKeyAttrNameAndValPairs>
ManagedObjectKeyAttrNameAndValPairs::=<attrName>=<attrValue>;<attrName>=<attrValue>

> **Note:**
>
> The MO_Detail parameter of a managed object instance is empty if there is one alarm only on a device.

Table B-2   SNMP trap fault notification example from a managed object

Information About Managed Object Instance	Description
Fan.nnc_srv_1;172.30.80.0;location=middle	Alarm from the middle fan on a device at 172.30.80.0
SessionAgent.nnc_srv_1;172.30.80.100;name=sa-tge-1	Alarm from the session agent "sa-tge-1" on a device at 172.30.80.100
HotPlugablePort.nnc_srv_1;172.30.80.200;slot=01;port=01;presence=removed	Alarm from removing a physical port on a device at 172.30.80.200

Table B-2   (Cont.) SNMP trap fault notification example from a managed object

Information About Managed Object Instance	Description
`CPU.nnc_srv_1;172.30.80.0;apSys CPUUtil`	Alarm in apSysMgmtGroupTrap, apSysCPUUtil, type CPUUtil

Fault notification is in the form of a severity alarm that provides information about detected faults or abnormal conditions. The following table shows how SDM severity alarms map to ITU X.733 severity alarms used by a northbound network management system.

Table B-3   SDM Severity Alarm Mapping to ITU X.733 Severity Alarms

SDM Severity Alarms	ITU X.733 Severity Alarms
Emergency/Critical	Critical
Major	Major
Minor	Minor
Warning	Warning
Clear	Clear
Unknown	Indeterminate

Session Delivery Manager Northbound Interface Notification Objects

The Oracle Communications Session Delivery Manager MIB lists the following northbound notification traps generated by the SDM server.

Trap Event	Description
apEMSNodeID	The identifier for a Oracle Communications Session Delivery Manager node that appears on the navigation tree in the Active configuration area on the Discovery table in the Host Name/IP Address column.
apCentralStartTime	The time configured on the Oracle Communications Session Delivery Manager server when an event occurs.
apEMSDateTime	The time configured on the Oracle Communications Session Delivery Manager server when an event completes.
apEMSUser	The user initiating the function. If the function was automatically initiated by the Oracle Communications Session Delivery Manager application, the user is system.
apEMDeviceAddress	The address for a device being managed.