Oracle® Communications Tekelec Platform

Operations, Administration, and Maintenance (OAM) User's Guide

Release 5.7

E53463 Revision 01

February 2015

ORACLE®

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This section contains a brief description of the Operations, Administration, and Maintenance (OAM) feature. The contents include sections about the manual scope, audience, and organization; how to find related publications; and how to contact Customer Support for assistance.

Overview

This documentation:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides procedures for using the application interface
- Explains the organization of, and how to use, the documentation

Scope and Audience

This manual is intended for anyone responsible for configuring and administering the Operations, Administration, and Maintenance options. Users of this manual must have a working knowledge of telecommunications and network installations.

Manual Organization

This document is organized into the following chapters:

- *Administration* contains information about the administration of users, passwords, groups, sessions, and other OAM functions.
- *Configuration* contains information about the configuration of network elements, services, resource domains, servers, server groups, places, place associations and networks on the OAM.
- *Alarms and Events* contains information about viewing, exporting and generating reports on active and historical alarms and events in OAM.
- *Security Log* contains information on the security log files included with OAM.
- *Status and Manage* contains information on the status and management of network elements, servers, high availablility servers, databases, KPIs, processes, tasks, and files on the OAM.
- *Measurements* contains information on the measurement elements on the OAM.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

	DANGER: (This icon and text indicate the possibility of *personal injury*.)

⚠	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
⚠	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **`Applications`** tile.
   The **Applications Documentation** page appears.
3. Select **`Apps A-Z`**.
4. After the page refreshes, select the **`Communications`** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **`View`** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **`PDF`** link and select **`Save Target As`**.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

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

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

Chapter 2

User Interface Introduction

Topics:

This section describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction with an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

DSR GUI

In a DSR, the following Main Menu options are accessible from the System OAM (SOAM) server:

- Transport Manager
- Communication Agent
- SS7/Sigtran
- Diameter Common
- Diameter
- RBAR
- FABR
- Policy and Charging
- IPFE
- MAP-Diameter IWF
- CPA

The following Main Menu options are accessible from the Network OAM (NOAM) server:

- Communication Agent
- Diameter Common > Network Identifiers > MCCMNC, MCCMNC Mapping
- Diameter > Configuration for Topology Hiding,
- Network-wide Policy and Charging > Configuration components are configurable on the NOAM; some Configuration components are view-only on the SOAM. Policy and Charging > Maintenance components are accessible on the NOAM only.
- MAP-Diameter IWF

Bulk Import and Bulk Export functions appear on both OAMs, to be used for the data that can be configured on that OAM.

Most other Main Menu options are configurable from the Network OAM server and view-only from the System OAM server.

User Interface Elements

Table 2: User interface elements describes elements of the user interface.

Table 2: User interface elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.

Element	Location	Function
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner: • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates that a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • **Page Title Area**: Occupies the top of the work area. It displays the title of the current page being displayed, the date and time, and includes a link to context-sensitive help. • **Page Control Area**: Is located below the Page Title Area, and is used to show controls for the Page Area (this area is optional). When available for an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • **Page Area**: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is

Element	Location	Function
		provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Splash Page Welcome Message*.

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the NOAM and view-only on the SOAM; and some menu options are configurable only on the SOAM. See *DSR GUI*.

Note: Some features will not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Manage licenses and upgrades • Authenticate LDAP servers • Configure SNMP trapping services • Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes

Menu Item	Function
	• Services • Servers • Server Groups • Resource Domains • Places • Place Associations On the SOAM, allows the user to configure the NOAM list plus Interface and Port DSCP.
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status & Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, and data file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager	Allows the user to configure adjacent nodes, configuration sets, or transports; and edit transports.
Communication Agent	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	Allows the user to configure various users, groups, remote signaling points, links and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data.
Diameter Common	Allows the user to configure: • Network Identifiers: on the NOAM - MCC Ranges • Network Identifiers on the SOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile assignments The DSR Bulk Import and Export functions are available on both OAMs for the data that is configured on that OAM.
Diameter	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAM, Diameter Topology Hiding configuration

Menu Item	Function
	• On the SOAM, Diameter Configuration, AVP Dictionary and Troubleshooting for IDIH configuration; Diameter Mediation configuration: and Maintenance functions
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.

Policy and Charging
 	
(optional)
	On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRF Pools
	  • PCRF Sub-Pool Selection Rules
	  • Network-Wide Options
	• Online Charging DRA
	  • OCS Session State
	  • Realms
	  • Network-Wide Options
	• Alarm Settings
	• Congestion Options
	
	On the NOAM, allows the user to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Status

Menu Item	Function

	• Policy Database Query
	
	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRFs
	  • Binding Key Priority
	  • PCRF Pools
	  • PCRF Pool to PRT Mapping
	  • PCRF Sub-Pool Selections
	  • Policy Clients
	  • Site Options
	• Online Charging DRA
	  • OCSs
	  • CTFs
	  • OCS Session State
	  • Realms
	• Error Codes
	• Alarm Settings
	• Congestion Options

Gateway Location Application (Optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.
MAP-Diameter Interworking	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm

Menu Item	Function
	• Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
CPA (Charging Proxy Application) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • System Options • Message Copy • Session Binding Repository • SBR Subresource Mapping This is accessible from the SOAM only.
Help	Launches the Help system for the user interface.
Logout	Allows the user to log out of the user interface.

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the **Group Administration** page. The default group, **admin**, is permitted access to all GUI options and functionality. Additionally, members of the **admin** group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options will not appear on your screen if you do not have administrative permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing a password upon login. The System Login page also features a current date and time stamp and a customizable login message.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request.

Customizing the Login Message

Prior to logging in, the **System Login** page appears. You can create a login message that will appear just below the **Log In** button on the **System Login** page.

Figure 1: Oracle System Login

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

The next time you log in to the user interface, the login message text is displayed.

Accessing the DSR Graphical User Interface

In a DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you will access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control > Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

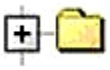
   When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.
   The System Login page appears.
3. Enter the Username and Password for your account.
   The DSR GUI for the NOAM appears.
4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.
   The DSR GUI for the SOAM appears.

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) will collapse the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.

Icon	Name	Description
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, you will see a variety of page formats. Tables, forms, tabbed pages, and reports are the most common formats in the user interface.

Note: Screenshots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination, with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.

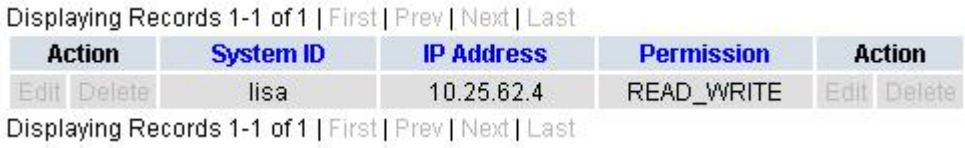


Figure 2: Paginated table

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see *Page Controls*.

Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	**31107**	**2009-Jun-11 18:07:24.704 UTC**	**MINOR**	**MiddleWare**	**inetmerge**	**SOAMP**	**teks8011002**	**COLL**	**teks8011004**	**DB merging from a child Source Node has failed**
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to

Export

Figure 3: Scrollable table

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of pulldown lists, buttons and links.

Username: Sample User Name (5-16 characters)
Group: Unassigned
Time Zone: UTC
Maximum Concurrent Logins: 1 Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]
Session Inactivity Limit: 120 Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range = 0-120]
Comment: guiadmin (max 64 characters)
Temporary Password: ●●●●●●● (8-16 characters)
Re-type Password: (8-16 characters)

Ok Apply Cancel

Figure 4: Form page

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields will populate on the page. Retrieve is always the default for tabbed pages.

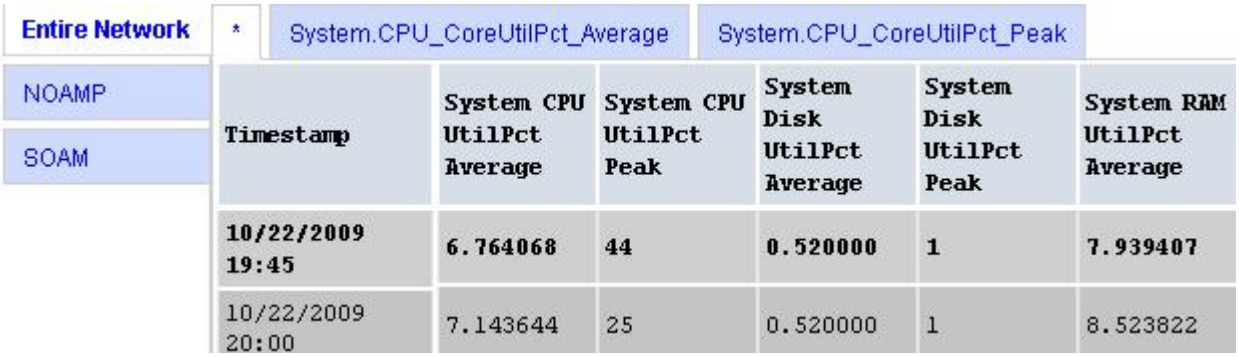


Figure 5: Tabbed pages

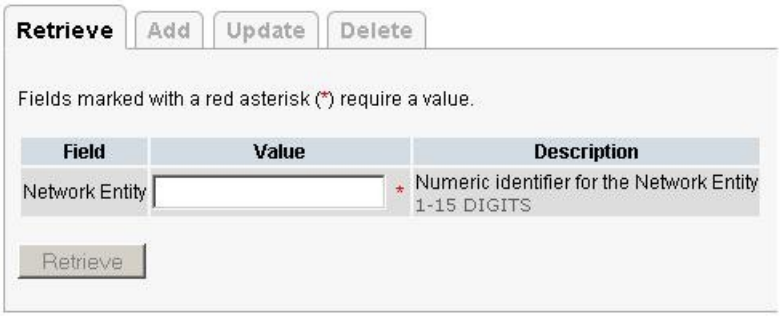


Figure 6: Tabbed pages

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking the **Report** button. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

```
==========================================================================================

User Account Usage Report

==========================================================================================

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin

------------------------------------------------------------------------------------------

Username          Date of Last Login    Days Since Last Login   Account Status
----------------  --------------------  ----------------------  ---------------
guiadmin          2009-06-19 19:00:17   0                       enabled

------------------------------------------------------------------------------------------

End of User Account Usage Report

==========================================================================================
```

Figure 7: Report output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the **User Interface** splash page appears. You can display a customized welcome message on the **User Interface** splash page. Use this procedure to customize the message.

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.
3. Enter the welcome message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

The next time you log in to the user interface, the welcome message text is displayed.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.

Local Node Name ▾	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set	IP Addresses

Figure 8: Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in **Group Administration**, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

Table 5: Example Action buttons contains examples of Action buttons.

Table 5: Example Action buttons

Action button	Function
Insert	Insert data into a table
Edit	Edit data within a table
Delete	Delete data from table
Change	Change the status of a managed object

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: Submit buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit buttons

Submit button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control is a widget that allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the **X** next to a pulldown list to clear the field.

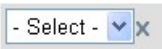


Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.

Figure 10: Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- Filter - Allows you to filter data in a table.
- Errors - Displays errors associated with the work area.
- Info - Displays information messages associated with the work area.
- Status - Displays short status updates associated with the main work area.
- Warning - Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 11: Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.
   The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see *Optional Layout Element Toolbar*.

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element - When enabled, the Network Element filter limits the data viewed to a single Network Element.

  Note: Once enabled, the Network Element filter will affect all pages that list or display data relating to the Network Element.

- Collection Interval - When enabled, the collection interval filter limits the data to entries collected in a specified time range.
- Display Filter - The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

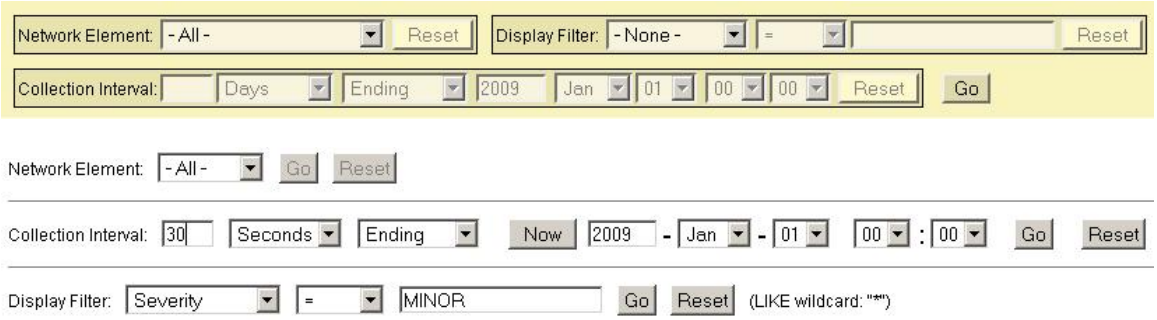


Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter control elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.

Operator	Description
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators will be available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.
   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.
   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes that you have a data table displayed on your screen. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Click **Filter** in the optional layout element toolbar.

The filter tool appears.

2. Select a field name from the **Display Filter** pulldown menu.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

   The selected field name displays in the **Display Filter** field.

3. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.

5. For data tables that support compound filtering, click the **Add** button to add another filter condition. Then repeat steps 2 through 4.
   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

   Note: MaxRecordsPerPage has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter 3

Administration

Topics:

This section describes administrative tasks. These tasks are at the system-level and are limited to users with administrative privileges. The associated menu items do not appear in the user interface for non-administrative users.

Options Administration

The **Options Administration** page enables the administrative user to view a list of global options.

General Options Administration elements

This table describes the elements of the **General Options Administration** page.

Table 8: General Options Administration Elements

Element	Description
LastLoginExpiration	Number of days of inactivity before a user account is disabled. (0 = never disable) [Default = 0; Range = 0-200] **Note:** This feature is not enabled by default.
LockoutWindow	Amount of time (in minutes) in which exceeding the maximum number of consecutive failed logins will cause an account to be locked out. (0 = unlimited)
MaxConsecutiveFailed	Maximum number of consecutive failed login attempts before account is disabled. (0 = never disable) [Default = 3; Range = 0-10]
MaxPasswordHistory	Maximum number of passwords maintained in history list before reuse of password is allowed. (0 = no password history) [Default = 3; Range = 0-10]
MaxRecordsPerPage	The maximum number of records to display per page [Default = 20; Range = 10-100]
PasswordExpiration	Time (in days) before passwords expire (0 = never) [Default = 90; Range = 0-90]
SAMLEnabled	Enables SAML authentication of users. (0 = disabled, 1 = enabled). [Default = 0]
SAMLInactivityTimeout	The time (in minutes) before SAML authenticated sessions expire. (Range = 0 to 3600, 0 means no expiration). [Default = 120]
SSOSessLife	Time (in minutes) before Single Sign-on Session expires [Default = 120]

Element	Description
WanBulkLoadLimit	Maximum number of allowed simultaneous WAN based bulk loads. [Default = 1; Range = 1-2]
DurableAdminState	The durability state of the system where: • 1 = NO disk (data is replicated to the active NO only) • 2 = NO pair (data is replicated to both the active and standby NOs) • 3 = NO Disaster Recovery NO (data is replicated to the active and standby NOs, as well as the secondary NO) [Default = 1; Range = 1-3]
DisabledAccount	Message displayed when attempting to login to a disabled account
FailedLoginMessage	Message displayed on failed login
IpAuthDeniedMessage	Configurable portion of IP Authorization Denied message
LoginMessage	Configurable portion of login message seen on the login screen
WelcomeMessage	Welcome message seen after successful login.
exportDataSpaceReplace	Replace a space in an export data filename or directory.(Default = underscore)

Viewing options

Use this procedure to view a list of global options:

Select **Administration > General Options**.

The **General Options Administration** page appears. The **General Options** pane lists all global options on the system. You can view the details of each option.

Updating a current global option

Use this procedure to update a global option.

1. Select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate the option you want to change.
3. Change the value of the option.
4. Click **OK** or **Apply** to submit the information.

This submits the information, updates the database tables, and allows you to input additional data.

The global option is changed.

Access Control

The Access Control page enables you to perform functions such as adding, modifying, enabling, or deleting user accounts, passwords, groups, sessions, single sign-on certificates, IPs and SFTP user information.

Users administration

The **Users Administration** page enables you to perform functions such as adding, modifying, enabling, or deleting user accounts.

Each user who is allowed access to the user interface is assigned a unique **Username**. This **Username** and the associated password must be provided during login. After three consecutive, unsuccessful login attempts, a user account is disabled. The number of failed login attempts before an account is disabled is a value that is configured through **Administrations > Options**. For more information, see *Options Administration*.

Each user is also assigned to a **group or groups**. Permissions to a set of functions are assigned to each group. The permissions determine the functions and restrictions for the users belonging to the group.

A user must have user/group administrative privileges to view or make changes to user accounts or groups. The administrative user can set up or change user accounts and groups, enable or disable user accounts, set password expiration intervals, and change user passwords.

Insert New User elements

The **Insert User** page displays the following elements:

Table 9: User Administration Elements

Element	Description	Data Input Notes
Username	A field for the Username. The Username allows access to the GUI and must be unique.	Format: String Range: 5-16 lowercase alphanumeric characters (a to z, 0 to 9)
Group	The groups to which the selected Username is assigned. Groups define the permissions assigned to the user. The permissions determine the functions and restrictions for the users belonging to the group.	Range: provisioned groups Default: admin

Element	Description	Data Input Notes
Authentication Options	Authentication options used with the account. When using local authentication, the account is disabled until a password is established. If using remote authentication, an authentication server must be configured.	Format: Checkbox Range: Allow Remote Auth or Allow Local Auth Default: Local Auth enabled, Remote Auth disabled
Access Allowed	Whether the user account is enabled.	Format: Checkbox Default: Account Enabled
Maximum Concurrent Logins	Maximum concurrent logins per user per server.	This feature cannot be enabled for users belonging to the admin group. Range: 0-50 Default: 0 0 = no limit
Session Inactivity Limit	The time, in minutes, after which login session expires.	Range: 0-3600 Default: 120 0 = session never expires
Comment	A field for user-defined text about this account (100 character maximum). This field is optional.	Format: Alphanumeric characters Range: 0-100 characters

Adding a new user

Note: Prior to performing this procedure, you should know to which user groups this user should be assigned. The group assignment determines the functions that a user has access to. If you need to create a new group for this user, you should do so prior to adding the user (see *Adding a group*).

Use this procedure to add a new user who will be allowed to log in to the user interface and access all or some of its functions:

1. Select **Administration > Users**.

   The Users administration page appears.

2. Click **Insert**.

   The Insert User Page appears.

3. Enter a **Username** that consists of 5-16 characters.

   For more information about **Username**, or any field on this page, see *Insert New User elements* .

4. Select a **Group** or **Groups** for the user.
5. Select the **Authentication Options** to be used with this account.

6. Select whether the account is enabled using the **Access Allowed** checkbox.
7. Enter the **Maximum Concurrent Logins**.

   Note: Maximum Concurrent Logins cannot be enabled for users in the admin group.

8. Enter the **Session Inactivity Limit**.
9. Enter text about this user in the **Comment** field.

   This field is required.

10. Perform one of the following actions:
    - Click **Apply**.

      A confirmation message appears at the top of the **Insert Users** page to inform you that the new user has been added to the database. To close the Insert Users page, click **Cancel**.

    - Click **OK**.

      The **Users administration page** re-appears with the new user displayed.

The new user is added to the database.

User Administration elements

The **User Administration** page displays the following elements:

Table 10: User Administration Elements

Element	Description
Username	The currently selected Username. The Username allows access to the GUI and must be unique.
Account Status	Enabled or disabled. If a user account is disabled, the user is unable to log in until an administrative user manually enables the account. If the user account is currently logged in, this action does not disrupt the session.
Remote Auth	Whether remote authorization is enabled or disabled.
Local Auth	Whether local authorization is enabled or disabled.
Consecutive Failed Login Attempts	The number of consecutive failed login attempts.
Concurrent Logins Allowed	The number of concurrent logins allowed.
Inactivity Limit	The limit set on account inactivity after login.
Comment	An optional field for user-defined text about this account (64 character maximum).
Groups	The groups to which the selected Username is assigned. Also provides a pull down list of

Element	Description
	provisioned groups. A user's groups determine the permissions assigned to the user. The permissions determine the functions and restrictions for the users belonging to the group.

Viewing user account information

Use this procedure to view user account information.

1. Select **Administration > Users**.

   The **Users Administration** page appears with the user account information displayed.

2. To view more detailed information, select **Report.**
   The Users Report displays with detailed information on the user account.

Updating user account information

Use this procedure to update user account information on the user interface:

1. Select **Administration > Users**.

   The **Users administration** page appears.

2. Select a user from the listing.
3. Select **Edit.**
4. Modify one or more of the user account information fields.
5. Click **Ok** or **Apply**.

   The **Users administration** page re-appears. The user account information is updated in the database, and the changes take effect immediately.

Deleting a user

Use this procedure to delete a user from the database. The next time the user attempts to log in, the user will be unable to log in. If the user is currently logged in to the system, this operation will not disrupt the user's current session. To stop a current user session, see *Deleting user sessions*, or to disable a user's account, see *Enabling or disabling a user account*.

1. Select **Administration > Users**.

   The **Users administration** page appears.

2. Select the appropriate user from the listing.
3. Click **Delete**.

   A confirmation box appears.

4. Click **OK** to delete the user.
   The **Users administration** page re-appears.

The user has been deleted from the database and no longer appears in the **Username** menu.

Enabling or disabling a user account

The user interface automatically disables a user account after five consecutive failed login attempts. The administrative user can also manually disable a user account to prevent a user from logging on to the system. If a user account is disabled, the user is unable to log in until an administrative user manually enables the account.

Use this procedure to enable or disable a user account:

1. Select **Administration > Users**.

   The **Users administration** page appears.

2. Select a **Username** from the listing.
3. Select **Edit.**
   The Edit Users page appears.
4. Click the **Account Enabled** checkbox to enable/disable the account. A check mark indicates that the account is enabled.
5. Click **Ok**.

   The account is enabled/disabled as selected.

Changing a user's assigned group

Use this procedure to change a user's assigned groups. The group assignment determines the functions that a user has access to (see *Groups Administration*). The next time the user logs in, the new assignment takes effect. If the user is currently logged in to the system, this operation will not affect the user's current session.

1. Select **Administration > Users**.

   The **Users Administration** page appears.

2. Select the appropriate user from the listing.
3. Select **Edit.**
   The Edit Users page appears.
4. Select the appropriate groups from the **Group** listing.
5. Click **Ok**.

The user's assigned groups are updated in the database and will take effect the next time the user attempts to log in to the user interface.

Generating a user report

A user account usage report can be generated from the **Administration > User** page. This type of report provides information about a user's account usage including last login date, the number of days since the user last logged in, and the user's account status. Use this procedure to generate a user account usage report.

1. Select **Administration > Users**.

   The **Users Administration** page appears.

2. Click **Report**.

   Note: It is unnecessary to select a particular user, because all users appear in the Users Report.

   The Users Report is generated. This report can be printed or saved to a file.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Passwords

Password configuration, such as setting passwords, password history rules, and password expiration, occurs in **Administration**. The application provides two ways to set passwords: through the user interface, see *Setting a password from the Users Administration page*, and at login, see *Setting a password from the System Login page*.

The user interface provides two forms of password expiration. The administrative user can configure password expiration on a system-wide basis. By default, password expiration occurs after 90 days. The administrative user can also disable the password expiration function. For procedural information on configuring password expiration, see *Configuring the expiration of a password*.

Password expiration is also forced the first time a user logs in to the user interface. During initial user account setup, the administrative user grants the user a temporary password. When the user attempts to log in for the first time, the software forces the user to change the password. The user is redirected to page where the user must enter the old password and then enter a new, valid password twice.

A valid password:

- must contain from 8 to 16 characters.
- must contain at least three of the four types of characters: numerics, lower case letters, upper case letters, or special characters (! @ # $ % ^ & * ? ~).
- cannot be the same as the Username or contain the Username in any part of the password (for example, **Username=jsmith** and **password=$@jsmithJS** would be invalid).
- cannot be the inverse of the Username (for example, **Username=jsmith** and **password=$@htimsj** would be invalid).
- cannot contain three or more consecutively repeated characters, or three or more ascending or descending alpha-numeric characters in a row, for example, **1234, aaaa, dcba**.
- cannot reuse any of the last three passwords.

Setting a password from the Users Administration page

Use this procedure to change an existing user's password.

Note: Only an administrative user may use this procedure. For information about how a non-administrative user can change a password, see *Setting a password from the System Login page*.

1. Select **Administration > Users**.

   The **Users Administration** page appears.
2. Select the appropriate user from the listing.
3. Click **Change Password**.

   The **Set Password** page appears. The selected user appears in the **New Password** box.

4. Enter a password in the **New Password** and **Retype New Password** fields. For information on valid passwords, see *Passwords*.

   The system verifies that the values entered in both fields match.

5. Click **Continue**.

   A confirmation message appears.

6. Select **Administration > Users** to return to the User Administration page.

The password has been updated in the database and will take effect the next time the user attempts to log in to the user interface.

Setting a password from the System Login page

Use this procedure to change a existing, non-administrative user's password on login.

Note: This procedure is for non-administrative users. For information about how an administrative user can set a password, see *Setting a password from the Users Administration page*.

1. Select **Change password** checkbox on the **System Login** page.
2. Enter the user name and password.
3. Click **Login**.

   The **Password Change Requested** page appears.

4. Enter a password in the **New Password** and **Retype New Password** fields. For information on valid passwords, see *Passwords*.

   The system verifies that the values entered are valid and that both fields match.

5. Click **Continue**.
   The password has been updated in the database and will take effect the next time the user attempts to log in to the user interface.

You have now completed this procedure.

Configuring the expiration of a password

Use this procedure to change the variable that controls the length of time for password expiration:

1. Select **Administration > Options**.

   The **Configuration administration** page appears.

2. Locate **PasswordExpiration** in the **Variable** column.
3. Enter an integer in the **Value** column. The integer indicates the number of days that elapse before the password expires. To disable password expiration, enter **0**.
4. Click **OK** or **Apply** to submit the information.

The password expiration variable is changed to the new value.

Groups Administration

The **Groups Administration** page enables you to create, modify, and delete user groups.

A group is a collection of one or more users who need to access the same set of functions. Permissions are assigned to the group for each application function. All users assigned to the same group have the same permissions for the same functions. In other words, you cannot customize permissions for a user within a group.

You can assign a user to multiple groups. You can add, delete, and modify groups except for the *Pre-defined user and group* that come with the system.

The default group, **admin**, provides access to all GUI options and actions on the GUI menu. You can also set up a customized group that allows administrative users in this new group to have access to a subset of GUI options/actions. Additionally, you can set up a group for non-administrative users, with restricted access to even more GUI options and actions.

For non-administrative users, a group with restricted access is essential. To prevent non-administrative users from setting up new users and groups, be sure **User** and **Group** in the Administration Permissions section are unchecked. Removing the check marks from the Global Action Permissions section will not prevent groups and users from being set up. The following figure displays these sections of the **Group Administration** page.

Permissions:

Resource	View	Insert	Edit	Delete	Manage
Global Action Permissions	☐	☐	☐	☐	☐
Administration Permissions	☐	☐	☐	☐	☐
General Options	☐		☐		
Users	☐	☐	☐	☐	☐
Groups	☐	☐	☐	☐	
Sessions	☐			☐	
Certificate Management	☐	☐	☐	☐	
Authorized IPs	☐	☐	☐	☐	
SFTP Users	☐	☐	☐	☐	
Software Versions	☐				
ISO Deployment	☐		☐		☐
Software Upgrade	☐		☐		☐
Remote LDAP Authentication	☐	☐	☐	☐	
Remote SNMP Trapping	☐		☐		
Remote Export Server	☐	☐	☐	☐	☐
DNS Configuration	☐		☐		
Licenses	☐	☐			

Figure 13: Global Action and Administration Permissions

Each permission option check box on the **Groups Administration** page corresponds to a menu option on the GUI main menu or a submenu. If a check box is checked for a group, the group has access to this option on the menu. If a check box is not checked, the group does not have access to this option, and the option is not visible on the GUI menu.

These check boxes are grouped according to the main menu's structure; most folders in the main menu correspond to a block of permissions. The exceptions to this are the permission option check boxes in the Global Action Permissions section.

The Global Action Permissions section allows you to control all insert (**Global Data Insert**), edit (**Global Data Edit**), and delete (**Global Data Delete**) functions on all GUI pages (except User and Group). For example, if the **Network Elements** check box is selected (in the Configurations Permissions section), but the **Global Data Insert** checkbox is not selected, the users in this group cannot insert a new Network Element.

By default, all groups have permissions to view application data and log files.

Pre-defined user and group

The following user account and group are delivered with the system and cannot be deleted or modified.

Table 11: Pre-defined User and Group

User	Group	Description
guiadmin	admin	Full access (read/write privileges) to all functions including administration functions.

OAM Groups Administration permissions

This table describes the OAM groups administration permissions.

Table 12: OAM Groups Administration permissions

Permission	Description
Global Action Permissions	
Global Data View	Grants permission to view data in database tables.
Global Data Insert	Grants permission to insert or add data to database tables.
Global Data Edit	Grants permission to edit or modify data in database tables.
Global Data Delete	Grants permission to delete data from database tables.
Global Data Manage	Grants permission to manage data in database tables.
Administration Permissions	

Permission	Description
General Options	Grants permission to configure global options such as: • last login expiration • maximum consecutive failed login attempts • password history • maximum records per page • password expiration • configuration of the login message • configuration of the welcome message
Users	Grants permission to set up new users.
Groups	Grants permission set up user groups.
Sessions	Grants permission to view and delete sessions information.
Certificate Management	Grants permission to view, insert, edit and delete SSO certificates.
Authorized IPs	Grants permission to insert and delete authorized IP addresses.
SFTP Users	Grants permission to view, insert, edit and delete SFTP Users.
Software Versions	Grants permission to view software version data.
ISO Deployment	Grants permission to transfer ISO files to be used in server installations and upgrades.
Software Upgrade	Grants permission to prepare, initiate, monitor, and complete server software upgrades.
Remote LDAP Authentication	Grants permission to view, insert, edit and delete LDAP Authetication.
Remote SNMP Trapping	Grants permission to view and edit SNMP Trapping.
Remote Export Server	Grants permission to view, insert, edit, delete and manage remote export servers.
Configuration Permissions	
Network Elements	Grants permission to insert, edit, delete, lock or unlock Network Elements.
Resource Domains	Grants permission to view, insert, edit, and delete Resource Domains.
Servers	Grants permission to insert new servers or delete servers from the topology.

Permission	Description
Services	Grants permission to insert, edit and delete new services in the topology.
Server Groups	Grants permission to group provisioned servers by role, function, and redundancy model.
Places	Grants permission to view, insert, edit, and delete Places.
Networks	Grants permission to insert, edit, and delete new networks in the topology.
DSCP	Grants permission to view, insert, edit, and delete DSCP data.
Network Devices	Grants permission to insert, edit, and delete new network devices in the topology.
Network Routes	Grants permission to insert, edit, and delete new network routes in the topology.
Alarms & Events Permissions	
View Active Alarms	Grants permission to view active alarms.
View Event History	Grants permission to view alarm and event history.
SNMP Trap Log	Grants permission to view SNMP trap log.
Security Log Permissions	
View Security Log	Grants permission to view security logs from all configured servers.
Status & Manage Permissions	
Network Elements	Grants permission to view the status of Network Elements, as well as manage Customer Router Monitoring.
Servers	Grants permission to stop, reboot, and restart configured servers.
HA	Grants permission to view detailed HA status.
Database	Grants permission to disable provisioning to servers, inhibit database replication, perform backups, compare a database to an archive, and restore a database.
KPIs	Grants permission to view KPIs for all configured servers.
Processes	Grants permission to view details about server processes.

Permission	Description
Active Tasks	Grants permission to view details about long running tasks.
Scheduled Tasks	Grants permissions to view details about scheduled tasks.
Files	Grants permission to display the file list for a network entity.
Measurements Permissions	
Report	Grants permission to create and export measurement reports.

IPFE Group Administration permissions

Table 13: IPFE Configuration Permissions describes the IP Front End (IPFE) Group Administration permissions.

Table 13: IPFE Configuration Permissions

Permission	Description
Options	Allows a user to create, edit, view, and delete IPFE Options
Target Sets	Allows a user to create, edit, view, and delete Target Sets and IP List TSAs

Communication Agent Group Administration permissions

Table 14: Communication Agent Configuration Permissions and *Table 15: Communication Agent Maintenance Permissions* describe the Communication Agent (ComAgent) Group Administration permissions.

Table 14: Communication Agent Configuration Permissions

Permission	Description
Remote Servers	Allows a user to create, edit, view, and delete Remote Servers
Connection Groups	Allows a user to create, edit, view, and delete Connection Groups
Routed Services	Allows a user to create, edit, view, and delete Routed Services

Table 15: Communication Agent Maintenance Permissions

Permission	Description
Show Connection Status	Allows a user to display Connection Status
Change Connection Status	Allows a user to change Connection Status
Show Routed Services Status	Allows a user to display Routed Services Status

Permission	Description
Show HA Services Status	Allows a user to display HA Services Status

DSR Diameter Group Administration permissions

The following tables describe the DSR Diameter Group Administration permissions:

Table 16: Diameter Configuration Permissions

Permission	Description
Local Nodes	Allows a user to create, edit, view, and delete Local Nodes
Peer Nodes	Allows a user to create, edit, view, and delete Peer Nodes
Connection Configuration Sets	Allows a user to create, edit, view, and delete Connection Configuration Sets
Capacity Configuration Sets	Allows a user to create, edit, view, and delete Capacity Configuration Sets
Connections	Allows a user to create, edit, view, and delete Connections
Route Groups	Allows a user to create, edit, view, and delete Route Groups
Route Lists	Allows a user to create, edit, view, and delete Route Lists
Peer Routing Rules	Allows a user to create, edit, view, and delete Peer Routing Rules
Egress Throttle Groups	Allows a user to create, edit, view, and delete Egress Throttle Groups
Reroute on Answer	Allows a user to define sets of Diameter Application Ids and Result Code AVP values that trigger Request message rerouting when an Answer response is received from a peer
Application Routing Rules	Allows a user to create, edit, view, and delete Application Routing Rules
System Options	Allows a user to view and edit System Options
DNS Options	Allows a user to view and delete DNS Options
Application Ids	Allows a user to create, edit, view, and delete Application Ids
CEX Configuration Sets	Allows a user to create, edit, view, and delete CEX Configuration Sets
Message Priority Configuration Sets	Allows a user to create, edit, view, and delete Message Priority Configuration Sets
Egress Message Throttling Configuration Sets	Allows a user to create, edit, view, and delete Egress Message Throttling Configuration Sets
Peer Route Tables	Allows a user to create, edit, view, and delete Peer Route Tables and Peer Routing Rules
Routing Option Sets	Allows a user to create, edit, view, and delete Routing Option Sets

Permission	Description
Pending Answer Timers	Allows a user to create, edit, view, and delete Pending Answer Timers
CEX Parameters	Allows a user to create, edit, view, and delete CEX Parameters
Command Codes	Allows a user to create, edit, view, and delete Command Codes
Capacity Summary	Allows a user to view the Capacity Summary
MP Profiles	Allows a user to create, edit, view, and delete MP Profiles
Profile Assignments	Allows a user to create, edit, view, and delete DA-MP Profile Assignments
Message Copy Configuration Sets	Allows a user to create, edit, view, and delete Message Copy Configuration Sets
Reserved MCC Ranges	Allows a user to create, edit, view, and delete MCC Ranges
Application Route Tables	Allows a user to create and delete Application Route Tables; and view and edit Rules in the tables
Trusted Network Lists	Allows a user to create, edit, view, and delete Trusted Network Lists for Topology Hiding
Path Topology Hiding Configuration Sets	Allows a user to create, edit, view, and delete Path Topology Hiding Configuration Sets
S6a/S6d HSS Topology Hiding Configuration Sets	Allows a user to create, edit, view, and delete S6a/S6d HSS Topology Hiding Configuration Sets
MME/SGSN Topology Hiding Configuration Sets	Allows a user to create, edit, view, and delete MME/SGSN Topology Hiding Configuration Sets
Protected Networks	Allows a user to create, edit, view, and delete Protected Networks for Topology Hiding
Connection Capacity Dashboard	Allows a user to view the Connection Capacity Dashboard
Import	Allows a user to provision the DSR system from an ASCII CSV (Comma Separated Values) text file
Export	Allows a user to "export" the DSR configuration data into a CSV (Comma Separated Values) file of the same format

Table 17: Diameter Maintenance Permissions

Permission	Description
Route Lists	Allows a user to view priority, capacity, Route Group assignment, and status information for Route Lists
Connections	Allows a user to view Initiator, Local Node, Peer Node, MP Server Hostname, Application ID, Admin State, Operational Status, and Operational Reason information for Connections. This permission also provides the ability to enable and disable Connections.

Permission	Description
Egress Throttle Groups	Allows a user to view Admin State, Operational Status, Operational Reason, and other information for Egress Throttle Group Rate Limiting and Pending Transaction Limiting
Route Groups	Allows a user to view Peer Node assignment, capacity, percent, and status information for Route Groups
Peer Nodes	Allows a user to view connection, status, and operation reason information for Peer Nodes
Applications	Allows a user to view status for DSR Applications
DA-MP Status	Allows a user to view status for DA-MPs

Table 18: Diameter Mediation Permissions

Permission	Description
Rule Templates	Allows an operator to define Mediation Rule Templates
Enumerations	Allows an operator to view and edit Mediation Enumerations
Triggers	Allows an operator to view and edit Mediation Triggers
State & Properties	Allows an operator to set the state of a Rule Template and configure settings for a Rule Template
AVP Dictionary	Allows an operator to view the AVPs familiar to the system, add new AVPs, and change the definition of a basic AVP
Vendors	Allows an operator to view and add new vendors
Rule Sets	Allows an operator to define Mediation Rule Sets

Table 19: Diameter Diagnostics Permissions

Permission	Description
Test Connections Diagnose	Allows diagnosis of test messages on a test connection
Test Connections Report	Allows reporting of diagnostic results
MP Statistics (SCTP)	Allows network operators to retrieve per MP SCTP statistics for MPs hosting Diameter connections.

Policy DRA Group Administration permissions

Table 20: Policy DRA Configuration Permissions and *Table 21: Policy DRA Maintenance Permissions* describe the Policy DRA Group Administration permissions.

The **Administration > Group** GUI page displays permissions check boxes for all Policy DRA pages, both NOAM and SOAM pages.

- All of the permissions can be updated only on the NOAM **Administration > Group** page.
- All of the permissions can be viewed but not updated on the SOAM **Administration > Group** page.

Table 20: Policy DRA Configuration Permissions

Permission	Description
PCRFs	Allows a user to create, edit, view, and delete PCRFs
Binding Key Priority	Allows a user to assign Binding Key Priorities to Binding Key Types
Topology Hiding	Allows a user to create, edit, view, and delete Policy Clents from which PCRF names should be hidden
PCRF Pools	Allows a user to create multiple PCRF Pools, which are selected using the combination of IMSI and Access Point Name (APN)
PCRF Pool To PRT Mapping	Allows a user to view the list of PCRF Pools or Sub-Pools configured at the NOAMP and allows each to be mapped to a Peer Routing Table to be used when a new binding is created for the PCRF Pool
PCRF Sub-Pool Selection Rules	Allows a user to create, edit, and delete rules for selection of a PCRF Sub-Pool for a given PCRF Pool and Origin-Host value
Network-Wide/Site Options	Allows a user to set network-wide Policy DRA configuration from the NOAM
Options	Allows a user to view and edit Network-Wide Options and Site Options
Error Codes	Allows a user to view and edit Result Codes to be returned for Policy DRA error conditions
Alarm Settings	Allows a user to view and edit Alarm Settings
Congestion Options	Allows a user to view and edit Congestion Options

Table 21: Policy DRA Maintenance Permissions

Permission	Description
Policy SBR Status	Allows a user to view status for Policy SBRs
Binding Key Query	Allows a user to enter a Binding Key Type and Binding Key search value, and search for the specified Binding Key data

RBAR Group Administration permissions

Table 22: RBAR Configuration Permissions describes the Range-Based Address Resolution (RBAR) Group Administration permissions.

Table 22: RBAR Configuration Permissions

Permission	Description
Applications	Allows a user to create, edit, view, and delete Applications

Permission	Description
Address Resolutions	Allows a user to create, edit, view, and delete Address Resolutions
Address Tables	Allows a user to create, edit, view, and delete Address Tables
Addresses	Allows a user to create, edit, view, and delete Addresses
Destinations	Allows a user to create, edit, view and delete Destinations
Exceptions	Allows a user to create, edit, view, and delete Exceptions
System Options	Allows a user to view and edit RBAR System Options

FABR Group Administration permissions

Table 23: FABR Configuration Permissions describes the Full Address-Based Resolution (FABR) Group Administration permissions.

Table 23: FABR Configuration Permissions

Permission	Description
Applications	Allows a user to create, edit, view, and delete Applications
Exceptions	Allows a user to create, edit, view, and delete Exceptions
Default Destinations	Allows a user to create, edit, view and delete Default Destinations
Address Resolutions	Allows a user to create, edit, view, and delete Address Resolutions
System Options	Allows a user to view and edit RBAR System Options

CPA Group Administration permissions

Table 24: CPA Configuration Permissions describes the Charging Proxy Application (CPA) Group Administration permissions.

Table 24: CPA Configuration Permissions

Permission	Description
Cpa System Options	Allows a user to view and edit CPA System Options
Cpa Message Copy	Allows a user to view and edit Message Copy elements for CPA
Cpa Sbr	Allows a user to view and edit SBR elements

Service Broker Group Administration permissions

This table describes elements of the **Group Administration** page.

Table 25: EAGLE XG NP Query Router

Permission	Description
Configuration	Allows access to Service Broker configuration settings
Query	Allows users to query NP Query Router configuration tables
Maintenance	Allows access to maintenance tools including enabling/disabling NP Query Router

SSR Group Administration permissions

This table describes the SSR group administration permissions.

Table 26: SSR Configuration Permissions

Permission	Description
POPs	Grants permission to view, insert, and delete POPs.
Domains	Grants permission to view, insert, and delete Domains.
Option Profiles	Grants permission to view, insert, edit, and delete Option Profiles.
Defaults	Grants permission to edit default options.
SUA Signaling Gateways	Grants permission to view, insert, edit, and delete SUA Signaling Gateways.
DNS	Grants permission to view and edit DNS servers, and to view, insert, edit, and delete DNS cache pre-load records.
SIP Server	Grants permission to edit TCP and SCTP options.
CAPM	Grants permission to view, insert, and delete CAPM definitions and enumerations.
Internal Components	Grants permission to view, insert, delete, and view Internal Components.

Table 27: SSR Routing Permissions

Permission	Description
Route Service	Grants permission to view, insert, edit, and delete Route Services.
Routing Profile	Grants permission to view, insert, edit, and delete Routing Profiles.
Rules	Grants permission to view, insert, edit, and delete Routing Rules.
RS Prefix Screening	Grants permission to view, insert, edit, and delete RS Prefix Screening
NP Prefix Screening	Grants permission to view, insert, edit, and delete NP Prefix Screening.

Permission	Description
CAPM Tasks	Grants permission to view, insert, edit, and delete CAPM Routing Task rules.

Table 28: SSR Routing Permissions

Permission	Description
Clusters	Grants permission to view, insert, edit, and delete Clusters and to assign Servers to Clusters and Clusters to MPs.
Servers	Grants permission to view, insert, edit, and delete Servers for Load Balancing Clusters.
Routing Policies	Grants permission to view, insert, edit, and delete Load Balancer Routing Policies.
Monitoring	Grants permission to set Load Balancer monitoring options and to monitor Load Balancer servers.

Table 29: SIP Timer Permissions

Permission	Description
Sets	Grants permission to view, insert, edit, and delete SIP Timer Sets.

Table 30: SSR Maintenance permissions

Permission	Description
SUA Connection Status	Grants permission to view the status of SUA Connections.
Selective Logging	Grants permission to view and provision selective logging rules and rule assignments, to activate or deactivate selective logging, and to view and save logs to a file.
DNS Cache	Grants permission to view and flush the DNS cache and to add and delete DNS cache entries
IP Blacklist	Grants permission to view and flush the IP Blacklist and to add an IP Blacklist entry.
Heartbeat List	Grants permission to view and flush the Heartbeat List and to add and delete Heartbeat List entries.
TCP Connections	Grants permission to view the status of TCP connections.
SCTP Associations	Grants permission to view the status of SCTP Associations.
SSR Configuration status	Grants permission to view the status of SSR Configuration.

SS7/Sigtran Group Administration permissions

This table describes the SS7/Sigtran group administration permissions. The SS7/Sigtran group administration permissions are only available in products that use the SS7/Sigtran plug-in.

Table 31: SS7/Sigtran Configuration Permissions

Permission	Description
Adjacent Servers	Grants permission to view, insert, and delete Adjacent Servers.
Adjacent Server Groups	Grants permission to view, insert, edit, and delete Adjacent Server Groups.
Local Signaling Points	Grants permission to view, insert, edit, delete, and generate a report on Local Signaling Points.
Remote Signaling Points	Grants permission to view, insert, delete, generate a report, and view status on Remote Signaling Points.
Remote MTP3 Users	Grants permission to view, insert, delete, and view the status of Remote MTP3 Users.
Link Sets	Grants permission to view, insert, delete, generate a report, and view status of Link Sets.
Associations	Grants permission to view, insert, edit, delete, generate a report, and view status of Associations. Grants permission to view, insert, edit, and delete an Association Configuration Set.
Links	Grants permission to view, insert, delete, generate a report, and view status of a Link.
Routes	Grants permission to view, insert, edit, delete, generate a report, and view status of Routes.
SCCP Options	Grants permission to view and edit SCCP Options.
MTP3 Options	Grants permission to view and edit MTP3 Options.
M3UA Options	Grants permission to view and edit MTP3 Options.
Local Congestion Options	Grants permission to view Local Congestion Options.
Local SCCP Users	Grants permission to view, insert, delete, generate a report, and view status of the Local SCCP Users.

Table 32: SS7/Sigtran Maintenance permissions

Permission	Description
Local SCCP Users	Grants permission to view the status of Local SCCP Users and to enable and disable LSUs.
Remote Signaling Points	Grants permission to view the status of Remote Signaling Points and to reset the network status of routes.

Permission	Description
Remote MTP3 Users	Grants permission to view the status of Remote MTP3 Users and to reset the subsystem and point code status.
Link Sets	Grants permission to view the status of Link Sets.
Links	Grants permission to view the status of Links and to enable and disable Links.
Associations	Grants permission to view the status of Associations and to enable, disable, and block Associations.

Table 33: SS7/Sigtran Command Line Interface

Command Import	Grants permission to use the Command Import page.

UDR Group Administration permissions

The following table describes the UDR Group Administration permissions.

Table 34: UDR Group Administration Permissions

Permission Group	Description
UDR Configuration	
Provisioning Options	Allows a user to view and edit provisioning option settings.
UDRBE Options	Allows a user to view and edit UDRBE option settings.
Provisioning Connections	Allows a user to view, add, edit, and delete provisioning connections.
Subscribing Client Permissions	Allows a user to view, add, or delete subscribing client permissions.
UDR SEC	
Entity	Allows a user to view, add, edit, or delete an entity.
Interface Entity Map	Allows a user to view, add, or delete an interface entity map.
Entity Field Set	Allows a user to view, add, edit, copy, or delete an entity field set.
Entity Base Field Set	Allows a user to view, add, edit, copy, or delete an entity base field set.
Entity Definition	Allows a user to view, add, edit, or delete an entity field set.
UDR Maintenance	
Subscriber Query	Allows a user to perform a subscriber query.
Connections	Allows a user to view current external connections.
Command Log	Command Log: Allows a user to view command log history.

Permission Group	Description
Import Status	Allows a user to view the status of import operations.
Export Schedule	Allows a user to view, add, edit, or delete an export schedule.
Export Status	Allows a user to view the status of exports.
Subscribing Client Status	Allows a user to view the status of subscribing clients.

Adding a group

Use this procedure to add a new group:

1. Select **Administration > Group**.

   The **Group Administration** page appears.

2. Click **New**.

   The **Add Group** page appears.

3. Enter a unique name in the **Group** field for the new group, and optionally, in the **Description** field, enter text to describe the group.
4. To allow Insert, Edit, or Delete actions on all pages accessed from the GUI menu (except User and Group), check mark to select the desired global actions.
5. Check mark the remaining menu permissions to which you want this group to have access.

   Note: To quickly select all permissions, click **Check All**. **Check All** automatically selects all of the permissions in the section. **Clear All** automatically clears all permissions. For more information on the options displayed on the Group page, see *OAM Groups Administration permissions* .

6. Perform one of the following actions:
   - Click **Apply**.

     A confirmation message appears at the top of the **Add Group** page to inform you that the new group has been added to the database. To close the **Create User Group** page, click **Cancel**.

   - Click **OK**.

     The **Group Administration** page re-appears with the new group displayed.

     Note: The **Group Members** pane at the bottom of the page displays the entry **None** for a new group. If you would like to add users to the new group now, double-click **None** to launch the **Add User** page. See *Adding a new user* for more information.

The new group is added to the database.

Viewing members of a group

Use this procedure to view a list of usernames assigned to a group:

1. Select **Administration > Group**.

   The **Group Administration** page appears.

2. Select the appropriate group from the **Group** pulldown menu.
3. Scroll down if necessary to view the **Group Members** pane.

   The **Group Members** pane lists all usernames assigned to the selected group. You can click a username to access the **User Administration** page for the selected username.

A list of group members is displayed.

Modifying a group

You cannot modify a predefined group provided during installation. See *Pre-defined user and group* for more information on this group.

Use this procedure to modify a group:

1. Select **Administration > Group**.

   The **Group Administration** page appears.

2. Select the appropriate group from the **Group** pulldown menu.
3. Make the modifications. For information on permission options, see *OAM Groups Administration permissions* .
4. Click **Update**.

   The **Update** button grays out after the operation is performed.

The modifications are written to the database. The main GUI menu of the affected user(s) is not changed until the user logs out and back in to the system, or the user refreshes the menu (using the web browser's Refresh function). The change in accessibility to menu options for affected user(s) takes effect immediately.

Deleting a group

Note that you cannot delete a predefined group provided during installation. See *Pre-defined user and group* for more information on this group.

Use this procedure to delete a group:

1. Select **Administration > Group**.

   The **Group Administration** page appears.

2. Select the appropriate group from the **Group** pulldown menu.
3. Scroll to the **Group Members** pane at the bottom of the page.

   The **Group Members** pane lists all usernames associated with the group. If there are usernames associated with the group, you must delete the usernames or assign them to another group prior to deleting the group.

4. Perform these steps to remove any associated usernames from the group:
   a) Click a username. The **User Administration** page appears. The page is populated with data associated with the selected username.
   b) To delete the username, click **Delete User** and then **OK** to confirm the deletion.

c) To change the group assignment for the username, select a group from the **Group** pulldown menu and then click **Update**.
d) Select **Administration>Group** to return to the **Group Administration** page.
e) Perform these substeps until all usernames are removed from the **Group Members** pane. The**Group Members** pane displays **None** when all username associations are remove

5. Click **Delete**.

   A confirmation box appears.

6. Click **OK** to delete the group. The **Delete** button grays out after the operation is performed.

The group is removed from the database.

Sessions Administration

The **Sessions Administration** page enables the administrative user to view a list of current user sessions and to stop user sessions that are in progress. This function does not disable the user's login account. To end a user session that is in progress, delete the user session. For other methods of controlling user access to a system, see *Enabling or disabling a user account* and *Deleting a user*.

Sessions Administration elements

This table describes elements of the **Sessions Administration** page.

Table 35: Sessions Administration Elements

Element	Description
Sess ID	Shows a system-assigned ID for the session.
Expiration Time	Shows the date and UTC time the session will expire.
Login Time	Displays the UTC login time.
User	Displays the **Username** of the user logged in to the session.
Group	Displays the **Group** to which the user belongs.
TZ	Displays the user time zone: UTC.
Remote IP	Displays the IP address of the machine from which the user connected to the system.

Viewing user sessions

Use this procedure to view a list of user sessions:

Select **Administration > Session**s.

The **Sessions Administration** page appears. The **Sessions** page lists all active sessions on the system.

Deleting user sessions

Use this procedure to delete a user session.

Note: You cannot delete your own session.

1. Select **Administration > Sessions**.

   The **Sessions Administration** page appears.

2. Click to select the appropriate session from the table.

   To distinguish the appropriate session, locate either the Username or the IP address in the data string found in the **Value** field. For more information about data in the Value field, see *Sessions Administration elements* .

   Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold**Ctrl** as you click to select specific rows.

3. Click **Delete**.

   The session is deleted, and the user is no longer logged in to the system. The next time the user attempts to perform an action, the user is redirected to the **System Login** page.

Certificate Management

The Certificate Management feature allows users to configure certificates for:

- HTTPS/SSL - allows secure login without encountering messages about untrusted sites
- LDAP (TLS) - allows the LDAP server's public key to encrypt credentials sent to the LDAP server
- Single Sign-On (SSO) - allows users to navigate among several applications without having to re-enter login credentials

When setting up Certificate Management, you must first assign a system domain name for the DNS Configuration before importing any certificates. For more information, see the topic on Adding a DNS Configuration.

After assigning a system domain name, you must configure the LDAP authentication servers used for single sign on. For more information, see the topic on Configuring LDAP Authentication Servers.

Configuring single sign-on zones

The following sections outline the information necessary to configure the single sign-on zones. This includes zone elements and procedures on configuring, updating, viewing and deleting zone information.

Single sign-on zone elements

Establishing the single sign-on zone

Re-establishing the single sign-on local zone

Deleting a single sign-on zone

Generating a Single Sign-On Zones Report

Single sign-on zone elements

The following element is used when configuring single sign-on zones:

Table 36: Single Sign-On Zone Element

Element	Description	Data Input Notes
Zone Name	Name of the SSO-compatible remote zone	Range: A to Z, a to z, 0-9 and periods - maximum 15 characters

Establishing the single sign-on zone

Before configuring a single sign-on zone, the single sign-on domain name must be configured.

Use this procedure to configure the single sign-on zone:

1. Select **Administration > Access Control > Certificate Management**.

   The Establish SSO Zone page appears.

2. Select the **Establish SSO Zone** button at the bottom of the table.

   The **Establish SSO Zone** page appears.

3. Enter a **Zone Name** that consists of 1-15 characters.
4. Select **Apply** to save the changes you have made and remain on this screen, or select **OK** to save the changes and return to the Zones page.

The new single sign-on zone is added to the database.

Re-establishing the single sign-on local zone

Re-establishing the local zone renders all of the certificates for this zone obsolete. After re-establishing the local zone, you will have to re-distribute the certificate for this zone to all the other remote zones in order to re-establish the trusted relationship and re-enable single sign-on between the zones.

Use this procedure to re-establish the single sign-on local zone:

1. Select **Administration > Access Control > Certificate Management**.

   The **Certificate Management** page appears.

2. Select the local zone from the listing.
3. Click **Reestablish Local Zone**.
   A confirmation message appears stating that reestablishing a local zone will invalidate configured SSO key-exchanges involving this machine.
4. Select **OK** to continue

The local zone is re-established in the database.

Deleting a single sign-on zone

Use this procedure to delete the single sign-on remote or local zone:

1. Select **Administration > Access Control > Certificate Management**.
2. Select the appropriate zone from the table listing.
3. Click **Delete**.

A confirmation box appears.

4. Click **OK** to delete the zone.

The zone is deleted from the database and no longer appears in the table listing.

Generating a Single Sign-On Zones Report

Use this procedure to generate a single sign-on zones report:

1. Select **Administration > Access Control > Certificate Management**.
2. Click to select the zone for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.
   The single sign-on zones report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Create CSR

The Certificate Management feature allows users to build certificate signing requests (CSRs)

A Certificate Signing request is a block of encrypted text that is generated on the single sign-on server. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country.

Create CSR elements

The following elements are used when creating a CSR:

Table 37: Create CSR Elements

Element	Description	Data Input Notes
Country	The 2-letter country code of which the entity being described lives in	Range: A to Z
State or Province	The state or province (full name) which the entity being described lives in	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens
Locality	The locality name (eg. city) of the entity being described	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens.
Common Name	The common name of the entity being described. Replacing a certificate marked visible or active will result in the browser connection errors - which may then require a reload or restart of the browser to restore connectivity. The list includes only those entities that do not	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens

Element	Description	Data Input Notes
	already have an associated certificate.	
Organization	The name of the organization which the entity belongs to	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens
Organizational Unit	The organizational unit name (eg. section) which the entity belongs to	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens
Email Address	The email address of the entity being described.	Range: 1-100 character long string. Allowed characters are A-Z, a-z, 0-9, '.', and '@'

Creating a CSR

The following sections outline the information necessary to create a CSR. A CSR is a certificate signing request, and is sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

1. Select **Administration > Access Control > Certificate Management**.

   The Certificate Management page appears.

2. Click **Create CSR**.
3. Select a two-character **Country** code for the entity.

   For more information about any field on this page, see CSR elements.

4. Select the full name of the **State or Province**.
5. Select the **Locality** name, for example, the city.
6. Select the **Common Name** for the entity being included in the CSR.
7. Select the entity **Organization**.
8. Select the entity **Organizational Unit** for the entity being included in the CSR.
9. Select the entity **Email Address**.
10. Click **Generate CSR** to submit the information.
11. Click **Back** to return to the Certificate Management page. The CSR displays in the table.

Import Certificate

The Certificate Management feature allows users to import certificates in cases where this is preferred over configuring certificates. All imported certificates are appended to the Certificate Management table.

Import Certificate elements

The following elements are used when importing a certificate:

Table 38: Import Certificate Elements

Element	Description	Data Input Notes
X.509 Certificate	PEM encoded X.509 certificate	Range: 2048 characters
Private Key	PEM encoded Private Key	Range: 2048 characters
Passphrase	The passphrase used to protect the Private Key	

Importing a Certificate

The following steps outline the procedures necessary to import a certificate.

1. Select **Administration > Access Control > Certificate Management**.

   The Certificate Management page appears.

2. Click **Import**.
3. Enter the **X.509 Certificate**.
   For more information about any field on this page, see Import Certificate elements.
4. Enter the **Private Key**.
5. Enter the **Passphrase**.
6. Click **OK** to import the certificate.

Deleting a Certificate

Use this procedure to delete a certificate:

1. Select **Administration > Access Control > Certificate Management**.
2. Select the appropriate certificate from the table listing.
3. Click **Delete**.

   A confirmation box appears.

4. Click **OK** to delete the certificate.

The certificate is deleted from the database and no longer appears in the table listing.

Generating a Certificate Report

Use this procedure to generate a certificate report:

1. Select **Administration > Access Control > Certificate Management**.
2. Click to select the certificate for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.
   The certificate report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Authorized IPs

IP addresses that have permission to access the GUI can be added or deleted on the **Authorized IPs** page. If a connection is attempted from an IP address that does not have permission to access the GUI, a notification appears on the GUI.

Note: This feature cannot be enabled until the IP address of the client is added to the authorized IP address table. You must add the IP address of your own client to the list of authorized IPs first before you enable this feature.

Authorized IPs elements

This table describes the elements on the **Authorized IPs** page.

Element	Description
IP Address	IP address with permission to access the GUI
Comments	Users can insert additional information (up to 64 characters) to describe the server, or the field can be left blank.

Enabling Authorized IPs functionality

Enabling Authorized IPs functionality prevents unauthorized IP addresses from accessing the GUI. Use this procedure to enable the Authorized IPs functionality.

Note: This procedure pertains to GUI access only.

1. Select **Administration > Authorized IPs**.
   The **Authorized IPs** page appears.

   Note: This feature cannot be enabled until the IP address of the client is added to the authorized IP address table. You must add the IP address of your own client to the list of authorized IPs first before you enable this feature.

   For more information, see *Inserting authorized IP addresses*

2. Select the Info box in the upper left corner of the screen and click **Enable**.
   The Authorized IPs functionality is enabled. Only authorized IPs can access the GUI.

Disabling Authorized IPs functionality

Use this procedure to disable the Authorized IPs functionality.

Note: This procedure pertains to GUI access only.

1. Select **Administration > Authorized IPs**.
   The **Authorized IPs** page appears.
2. Select the Info box in the upper left corner of the screen and click **Disable**.
   The Authorized IPs functionality is disabled.

Inserting authorized IP addresses

Use this procedure to insert authorized IP addresses.

Note: This procedure pertains to GUI access only.

1. Select **Administration > Authorized IPs**.
   The **Authorized IPs** page appears.
2. Click **Insert**.
   The **Authorized IPs Insert** page appears.
3. Enter an IP address in the **IP Address Value** field.

   For more information about the **IP Address Value**, or any field on this page, see *Authorized IPs elements* .
4. Enter a comment in the **Comment Value** field.

   Note: This step is optional.
5. Do one of the following:
   - Click **OK**.

     The **Authorized IP** page reappears, and the IP address you entered is visible in the table. The IP address is authorized to access the GUI.
   - Click **Apply**.

     The IP address you entered is authorized to access the GUI. You can now enter additional IP addresses. Click **Apply** after each IP address entered. When you have finished entering IP addresses, click **OK** to return to the **Authorized IPs** page. All of the IP addresses you entered are visible in the table.

Deleting authorized IP addresses

Use this procedure to delete authorized IP addresses.

1. Select **Administration > Authorized IPs**.
   The **Authorized IPs** page appears.
2. Click to select the IP address you want to delete from the Authorized IP Address table.

   Note: Do not delete your own IP address. If you delete your own IP address, you will lose access to the GUI. If this happens, contact the Customer Care Center.
3. Click **Delete**.
   A delete confirmation message appears in a pop up window.
4. Click **OK**.
   This deletes the IP address from the table, and the IP address no longer has permission to access the GUI when the feature is enabled.

You have now completed this procedure.

SFTP Users Administration

The SFTP Users feature adds the ability to configure remote access accounts for SFTP access, and provide restricted access through those accounts to the export area of the file management directory to use for exporting MEAL data.

SFTP User elements

This table describes the elements on the SFTP Users page.

Element	Description
Username	The SFTP user name account. Range = Lowercase alphanumeric (a-z, 0-9) string between 5 and 32 characters long.
Permissions	The permissions associated with the account. The user will only access export files that match the assigned permission. Valid permissions are: • Measurements, Alarms and Events • Security Logs • Measurements, Alarms, Events and Security Logs
Comment	Comments about the SFTP user. Range = A string between 1 and 100 characters long.
SSH Key	The SSH public key to be used with this account.

Adding a SFTP User

Use this procedure to add a SFTP user:

1. Select **Administration > SFTP**.

   The SFTP Administration page appears.

2. Select **Insert.**
3. Enter a **username** to be used to identify the SFTP User.

   For more information about any field on this page, see SFTP User Elements.

4. Select the **permissions** to be associated with the SFTP user.
5. Enter a **comment**, if necessary, about the SFTP User.
6. Enter the **SSH public key** to be used with the account.
7. Click **OK** to submit the information and return to the SFTP Administration page, or click **Apply** to submit the information and continue entering additional data.

The new SFTP user information and related settings are saved and activated.

Viewing SFTP Users

Use this procedure to view SFTP user information.

Select **Administration > SFTP User**.

The **SFTP Users** page appears. The **SFTP** page lists all SFTP options on the system.

Updating SFTP User information

Use this procedure to update SFTP user information:

1. Select **Administration > SFTP Users**.

   The SFTP Users page appears.

2. Update SFTP settings as needed.
3. Click **OK** or **Apply** to submit the information.

The SFTP user changes are saved and activated.

Showing SFTP User Logs

A SFTP user access log can be generated. Use this procedure to generate a SFTP user access log.

1. Select **Administration > Access Control > SFTP User**.

   The SFTP Users page appears.

2. Highlight a user from the listing and click **Show Logs**.
   The SFTP Users log is generated showing all activity for the user. This report can be printed or saved to a file.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Deleting a SFTP User

Use this procedure to delete a SFTP user:

1. Select **Administration > Access Control > SFTP Users**.

   The SFTP Users page appears.

2. Select the appropriate user name from the listing for the SFTP user to delete.
3. Click **Delete**.

   A confirmation box appears.

4. Click **OK** to delete the user.
   The SFTP Users page re-appears.

The user is deleted from the database and no longer appears in the listing.

Generating a SFTP User report

A SFTP user report can be generated. Use this procedure to generate a SFTP user report.

1. Select **Administration > Access Control > SFTP User**.

   The SFTP Users page appears.

2. Click **Report**.

   Note: It is unnecessary to select a particular user, because all users appear in the Users Report.

   The SFTP Users report is generated. This report can be printed or saved to a file.

3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Showing SFTP User Logs

A SFTP user access log can be generated. Use this procedure to generate a SFTP user access log.

1. Select **Administration > Access Control > SFTP User**.

   The SFTP Users page appears.

2. Highlight a user from the listing and click **Show Logs**.
   The SFTP Users log is generated showing all activity for the user. This report can be printed or saved to a file.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Updating SFTP User password settings

Use this procedure to update SFTP user password settings:

1. Select **Administration > SFTP Users**.

   The SFTP Users page appears.

2. Select a user from the listing and select **Change Password.**
   The SFTP Users [Change Password] screen displays.
3. Enter the new SFTP password for this user. Confirm the entry by retyping the password.

   Note: Passwords must contain at least three of the following characters to be valid: numeric, lowercase letters, uppercase letters, or a special character.

4. Select **Continue** to save the password information.

The SFTP user password changes are saved and activated.

Software Management

The Software Management options allow you to administer:

- Versions
- Upgrade

For more information, see each individual section.

Versions

The **Versions** page is a report that displays the software release levels for the server. The report can be viewed on the screen, printed, or saved to a file.

Printing and saving the Software Versions report

Use this procedure to print or save the Software Versions report.

1. Select **Administration > Software Management > Versions**.
   The **Versions** page appears.
2. Click **Print** to print the report.
   A **Print** window appears. Click **OK**.
3. Click **Save** to save the report to a file.

You have now completed this procedure.

ISO Administration

The **ISO Administration** page controls the validation and transfer of the ISO file to all servers during a software installation or upgrade. An ISO file must first exist in the file management area of the network OAMP server before it can be validated or transferred. Use the procedure *Uploading a local file* to copy the ISO file to the file management area.

WARNING

Warning: Contact Technical Services and inform them of your upgrade plans prior to beginning any upgrade procedure.

ISO Administration elements

This table describes the elements on the **ISO Administration** page.

Table 39: ISO Administration Elements

Element	Description	Data Input Notes
System Name/ Hostname	The systems configured on the **Configuration > Systems** page.	Range: All configured System Names/ Hostnames
ISO	The last ISO file name successfully transferred to each System Name/Hostname during this GUI session.	Range: No Transfer in Progress, <ISO filename>

Element	Description	Data Input Notes
Transfer Status	The status of the ISO file transfer for each System Name/ Hostname. A transfer In Progress for a server appears with a yellow background, transfer Complete with a green background, and transfer Failed with a red background.	Range: N/A, In Progress, Failed, Complete

Viewing ISO transfer status

Use this procedure to view the configured Systems and the status of ISO file validation/transfer for each.

Select **Administration > Software Management > ISO Deployment**.

The **ISO administration** page appears. The **ISO** table lists all configured systems/ hostnames, and the validation/transfer status of each for this GUI session.

ISO transfer elements

This table describes the elements on the **ISO Transfer** page.

Table 40: ISO Transfer Elements

Element	Description	Data Input Notes
Select ISO to Transfer	List of ISO files in the file management area of the active NO server.	Format: Pulldown list Range: All available ISO files
Select Target System(s)	List of systems/servers.	Format: List box Range: All configured Systems Names/ Hostnames
Perform Media Validation before Transfer	Specifies whether or not to validate the ISO file at the network OAMP before the transfer begins. The validation process checks the ISO image for corruption.	Format: Check box Range: Selected or unselected Default: Selected

Transferring ISOs

The GUI provides the capability to transfer ISO files from the file management area of the active network OAMP server to one or more servers. Use this procedure to transfer an ISO.

1. Select **Administration > Software Management > ISO Deployment**.

   The **ISO Administration** page appears.

2. Click **Transfer ISO**.

   The **ISO Transfer** page appears.

3. Select the ISO file to transfer from the **Select ISO to Transfer** pulldown list.
4. Click to select the target systems or servers for the ISO file. To select more than one system or server, press and hold the **Ctrl** key when clicking to select.
5. To perform media validation, select the **Perform Media Validation before Transfer** check box.
6. Click **OK**.

Note: You cannot cancel once the validation/transfer process begins.

The **ISO administration** page appears again, with the status of the validation/transfer displayed in the green message box.

If **Perform Media Validation before Transfer** was selected, then the selected ISO file is validated at the network OAMP. If validation is successful, the file transfer begins. If validation fails, **Failed** appears in the **Transfer Status** column, an error appears in the message box (which is now red), and the transfer is aborted.

During the file transfer, **In Progress** appears in the **Transfer Status** field for the servers receiving the ISO file. To view a change in the **Transfer Status** for a server, you must click **Refresh** in the green message box. When the transfer is successfully completed, Complete appears in the **Transfer Status** field.

For a complete list of steps in the upgrade process, see the Upgrade procedure included in the Upgrade Kit.

Upgrade

The **Upgrade** page is used to perform a software upgrade on in-service servers in a network. Several steps in the upgrade process are required before using the **Upgrade** GUI option.

Warning: Contact the Customer Care Center and inform them of your upgrade plans prior to beginning any upgrade procedure.

Upgrade Administration elements

This table describes the elements on the **Upgrade Administration** page.

Table 41: Upgrade Administration Elements

Element	Description
Hostname	Lists the Hostname of the server.
Upgrade State	Displays the state that allows for graceful upgrade of server without degradation of service. Based on HA Status and Application State. Available states are: • Backup Needed

Element	Description
	• Backup in Progress • Ready • Pending • Upgrading • Accept or Reject • Failed • Backout Ready
Server Status	Overall server status. Selecting the link displays the full 'Server Status' report for the server.
OAM Max HA Role	The OAM maximum HA role for this server.
Appl Max HA Role	The application maximum HA role for the server.
Max Allowed HA Role	The maximum allowed HA role for the server.
Server Role	Role of this server in the system. Role is configured on the **Configuration > Server** page.
Network Element	Lists the Network Element to which the server belongs.
Function	Function of this server in the system. NOAMP and SOAM function are assigned on the **Configuration > Server** page. For message processors, function is assigned on the related configuration page.
Application Version	Application version currently installed and running on each server.
Upgrade ISO	The ISO used for the upgrade.
Start Time	The time upgrade started.
Status Message	The current upgrade status message.
Finish Time	The time upgrade finished.

Overview of the upgrade procedure

The information in this section is a general overview of the Upgrade page and what changes occur when you prepare a server for upgrade.

There is a recommended procedure to follow when upgrading a server:

1. Backup your server.
2. Do a cleanup of your ISO records (not required).
3. Prepare your server for upgrade.
4. Initiate an upgrade.
5. Complete the upgrade.
6. Accept the upgrade.

The sections that follow contain detailed information and steps for upgrading a server.

Caution: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, go to the My Oracle Support website and review any relevant Technical Service Bulletins (TSBs). Use only the upgrade procedure provided by My Oracle Support.

Caution: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

Backing up full configuration prior to an upgrade

It is recommended that you back up your server's full configuration prior to an upgrade. The configuration backup of a server runs in the background, enabling you to continue working while a backup is in process.

To backup a server prior to an upgrade:

1. Select **Administration > Software Management > Upgrade**.

   The **Upgrade** page appears.

2. (Optional) If you would like to selectively back up individual servers, highlight the server(s) from the listing. Prior to backup, the server must be in the **Backup Needed** or **Ready** state. If you would like to back up the entire server group, leave all servers unselected.
3. Select **Backup**.

   The **Upgrade (Backup)** form appears.

4. On the Upgrade (Backup) form, select **Exclude** (to perform a full backup of the COMCOL run environment, excluding the database parts specified in the files) or **Do Not Exclude** (to perform a full backup of the COMCOL run environment without excluding any database parts, which is a longer procedure and produces larger backup files).
5. Select **OK** to run the back up procedure.

The backup process saves server information in the background for either all the servers that are available for backup, or just for the selected server(s).

ISO Cleanup for upgrading servers

After backing up a server, it is recommended to clean up the ISO images for the server prior to a complete upgrade. This is not a required step, and if you do not trigger an ISO cleanup after back up, the system automatically cleans up the ISO images during the upgrade process.

Use the following steps to initiate an ISO cleanup:

1. Select **Administration > Software Management > Upgrade**.

   The **Upgrade** page appears.

2. Highlight the server(s) from the listing. Prior to ISO cleanup, the server must be in the **Not Ready** state.
3. Select **ISO Cleanup**.

4. Select **OK** on the confirmation screen to initiate the ISO cleanup.

The cleanup process deletes the ISO images for the selected server.

Preparing a server for upgrade

After backing up your server information and cleaning up your ISO images, the server must be prepared for the upgrade. Before a server can be upgraded it must be in the Ready state. This state allows the server to be upgraded. Preparing the server performs an Upgrade Ready Check with errors and warnings based on Upgrade Criteria.

The process of putting a server into the Ready state can take some time to complete, because processes have to shutdown gracefully. The page will refresh automatically and display updates to the server status as they become available.

As part of the transition to Ready state, the following changes occur:

- The server is placed in Forced Standby
- The application is Disabled
- On the **Upgrade Administration** page, Ready appears in the Upgrade State column.
- The **Initiate** and **Complete** buttons are enabled and the **Prepare** button is disabled when servers in the Ready state are selected.

  Note: Disabled buttons appear grayed out.

Use the following procedure to prepare the server for backup:

1. Select **Administration > Software Management > Upgrade**.

   The **Upgrade** page appears.

2. Highlight the desired server(s) from the listing.
3. Select **Prepare**. The Prepare Update page appears.
4. Select Prepare from the drop down listing next to the appropriate server name.
5. Select **OK**.

The system prepares the server for upgrade and returns the server to the listing with a Ready state.

Prepare Upgrade elements

This table describes the elements on the Prepare Upgrade form.

Table 42: Prepare Upgrade Elements

Element	Description
Hostname	The server hostname
Action	The action to take on the server. Default: Prepare. Range: Prepare, Do not prepare
Max HA Role	The Max HA Role of the server
Active Mates	The Active Mates of the server

Element	Description
Standby Mates	The Standby Mates of the server
Spare Mates	The Spare Mates of the server

Server Upgrade

Use the following procedure to initiate a server upgrade:

1. Select **Administration > Software Management > Upgrade**.

   The **Upgrade** page appears.

2. Select one or more servers by highlighting them from the list.
3. Select **Upgrade Server**.

   The **Initiate Upgrade** form appears.

4. Select the appropriate ISO image from the **Upgrade ISO** drop down list.
5. Select **OK**.

The system initiates the upgrade.

Initiate Server Upgrade elements

This table describes the elements on the **Initiate Upgrade** form for individual server upgrades.

Table 43: Initiate Upgrade elements (Individual Servers)

Element	Description
Top Section	
Hostname	Hostname of the server
Action	The action available during the upgrade. This field is not editable. Valid value is: • Upgrade
Status	The current status of the server. Includes: • OAM Max HA Role • Appl Max HA Role (MP server groups only) • Network Element • Application Version
Upgrade Settings Section	
Upgrade ISO	A drop down list that contains the file names of available ISO images.

Completing and accepting an upgrade

After backing up the server information, cleaning up the ISO images, preparing the server to be upgraded by changing the state to Ready, and initiating the upgrade, the upgrade must be completed and accepted. Completing an upgrade returns the server to the previous state and removes the Forced Standby. Accepting the upgrade confirms that the upgrade is correct and signals the end of the upgrade process.

Use the following procedure to complete an upgrade:

1. Select **Administration > Software Management > Upgrade**.

   The **Upgrade** page appears.

2. Highlight the server(s) from the listing.
3. Select **Complete**.
   The server returns to the Not Ready state and the application restarts. An alarm is sent to COMCOL and the Accept and Reject buttons are activated.
4. Confirm the need to upgrade the system files.

   Note: It is not necessary to select **Accept** in any timely fashion. The decision may be made to test the new upgraded system and confirm there is no need to revert before accepting the upgrade. Once an upgrade is accepted, the backup configuration files are deleted.

5. Select **Accept** to complete the upgrade.

The upgrade is complete.

Remote Servers

The Remote Servers options allow you to administer:

- LDAP Authentication
- SNMP Trapping
- Data Export
- DNS Configuration

For more information, see each individual section.

LDAP Authentication

The following sections outline the information necessary to configure the authentication or LDAP servers. This includes server elements and procedures on configuring, updating, viewing and deleting server information.

Single sign-on (SSO) can be configured to work either with or without a shared LDAP authentication server. If an LDAP server is configured, SSO can be configured to require remote (LDAP) authentication for SSO access on an account by account basis. The default user account (guiadmin) cannot be configured to use remote (LDAP) authentication.

If multiple LDAP servers are configured, the first available server in the list will be used to perform the authentication. Secondary servers are only used if the first server is unreachable.

If the system is not using a DNS server or IP address for the LDAP server, the LDAP server must be added to the etc/hosts file.

LDAP Authentication elements

This table describes the elements of the LDAP Authentication page.

Table 44: LDAP Authentication Elements

Element	Description	Data Input Notes
Hostname	Unique case-sensitive name for the server.	Format: Valid IPv4 or IPv6 address or a valid hostname. Format: Case-sensitivealphanumeric [a-z, A-Z, 0-9], period (.) and minus sign (-) . The first character must be alpha. Range: 1 to 255-character string
Account Domain Name	Domain name of the LDAP server.	Format: <name>.<tld> (ex. website.com). Range = 1-20 character alphanumeric [a-z, A-Z, 0-9], period (.)
Account Domain Name Short	The short version of the domain name listed above (ex.WEBSITE).	Must be a capitalized version of the domain name, without the extension. Range = 1-10 character alphanumeric [a-z, A-Z, 0-9]
Port	Port that the LDAP servers can be accessed by on the host machine	Default = 389 Range = Integer with value between 0 and 65535
Base DN	Directory path of the user being authenticated.	Range = 1-100 character alphanumeric [a-z, A-Z, 0-9]
Username	Username used for account DN lookups	Range = 1-15 character alphanumeric [a-z, A-Z, 0-9]
Password	The password of the user DN used for account lookups.	Range: restrictions depend on the LDAP server's settings.
Account Filter Format	User account search filter	Range = 1-100 character alphanumeric [a-z, A-Z, 0-9]

Element	Description	Data Input Notes
		Default = (&(objectClass=user)(sAMAccountName=%s))
Account Canonical Form	Canonical Form for the provided username	Format: Radio buttons Valid choices: • Traditional (e.g., guest) • Backslash (e.g., WEBSITE\guest) • E-Mail (e.g., guest@website.com) Default = Backslash style
Referrals	Whether or not to follow referrals	Default = unchecked (ignore)
Bind Requires DN	Whether the LDAP authentication bind requires a username in DN form	Default = unchecked (disabled)

Configuring LDAP authentication servers

Use this procedure to configure LDAP authentication servers:

1. Select **Administration > Remote Servers > LDAP Authentication**.
2. Click **Insert** at the bottom of the table.

   The **LDAP Authetication Insert** page appears.
3. Enter a **Hostname**. This is a user-defined name for the server. The hostname must be unique.
4. Enter an **Account Domain Name**. This is the name of the LDAP server.
5. Enter an **Account Domain Short Name**. This is a shorter version of the domain name, for example, WEBSITE.
6. Enter the **Port** for the LDAP server on the remote machine.
7. Enter the **Base DN**. This is the directory path of the user being authenticated.
8. Enter the **User Name** for the user domain name.
9. Enter the **Password** for the user domain.
10. Enter the **Account Filter Format**. This is the user account search filter.
11. Enter the **Account Canonical Form**. This is the format for the user name listing.
12. Select whether or not to follow **Referrals.**
13. Select whether or not to enable **Bind Requires DN**, which determines whether the LDAP required the user name in DN format.
14. Click **OK** to submit the information and return to the LDAP Authentication page, or click **Apply** to submit the information and continue entering additional data.

    Note: Once you have entered LDAP servers to the listing, you can order them using the **Move Up** and **Move Down** buttons on the LDAP Authentication screen. The server order in the listing determines the order that servers are tried against.

15. When finished adding LDAP servers, use the **Test Server** button to validate the server connection. This button allows you to confirm the server settings (by entering the correct userid/password combination) without logging out.

Updating LDAP Authentication Servers

Use this procedure to update LDAP authentication server information:

1. Select **Administration > Remote Servers > LDAP Authentication**.

   The **LDAP Authentication** page appears.

2. Update LDAP settings as needed.
3. Click **OK** or **Apply** to submit the information.

The LDAP server changes are saved and activated.

Generating a LDAP Authentication report

Use this procedure to generate a LDAP Authentication report.

1. Select **Administration > Remote Servers > LDAP Authentication**.

   The LDAP Authentication page appears.

2. Click **Report**.

   Note: It is unnecessary to select a particular user, because all users appear in the Users Report.

   The LDAP Authentication report is generated. This report can be printed or saved to a file.

3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Deleting a LDAP Authentication Server

Use this procedure to delete a LDAP Authentication server:

1. Select **Administration > Remote Servers > LDAP Authentication**.

   The **LDAP Authentication** page appears.

2. Select the appropriate host name from the listing for the LDAP Authentication server to delete.
3. Click **Delete**.

   A confirmation box appears.

4. Click **OK** to delete the authentication server.
   The **LDAP Authentication** page re-appears.

The server is deleted from the database and no longer appears in the listing.

SNMP Trapping

The GUI has an interface to retrieve key performance indicators (KPIs) and alarms from a remote location using the industry-standard Simple Network Management Protocol (SNMP). Only the Active Network server allows SNMP administration.

Note: The SNMP Manager is provided by the customer.

The SNMP agent is responsible for SNMP-managed objects. Each managed object represents a data variable. A collection of managed objects is called a Management Information Base (MIB). In other words, a MIB is a database of network management information that is used and maintained by the SNMP protocol. The MIB objects contain the SNMP traps that are used for alarms; a readable SNMP table of current alarms in the system; and a readable SNMP table of KPI data.

The Active Network server provides a single interface to SNMP data for the entire network. Alternately, functionality may be enabled that allows individual servers to send traps, in which case individual servers interface directly with SNMP managers.

Note: Note that only the Active Network server allows SNMP administration.

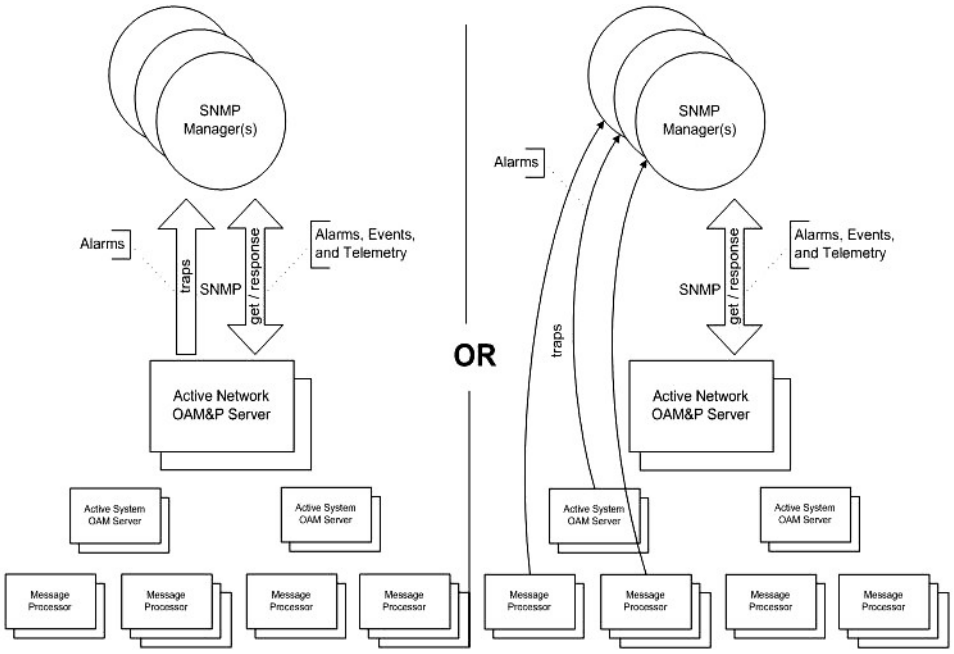


Figure 14: SNMP Support

The application sends SNMP traps to SNMP Managers that are registered to receive traps. IP addresses and authorization information can be viewed and changed using the SNMP administration page. For SNMP to be enabled, at least one Manager must be set up.

SNMP administration elements

On the active network OAM&P server, the **SNMP Administration** page provides for the configuration of SNMP services. This table describes the elements of the **SNMP Administration** page.

Table 45: SNMP Administration Elements

Element	Description	Data Input Notes
Manager 1	Manager to receive SNMP traps and send requests. It could be a valid IP address or a valid hostname.	Valid IP address or a valid hostname IP format: Four, 8-bit octets separated by periods [The first octet = 1-255; the last three octets = 0-255] Hostname Format: Alphanumeric [a-z, A-Z, 0-9] and minus sign (-) Hostname Range: 1 to 255-character string
Manager 2	Manager to receive SNMP traps and send requests. It could be a valid IP address or a valid hostname.	See description for Manager 1.
Manager 3	Manager to receive SNMP traps and send requests. It could be a valid IP address or a valid hostname.	See description for Manager 1.
Manager 4	Manager to receive SNMP traps and send requests. It could be a valid IP address or a valid hostname.	See description for Manager 1.
Manager 5	Manager to receive SNMP traps and send requests. It could be a valid IP address or a valid hostname.	See description for Manager 1.
Enabled Versions	Enables the specified version(s) of SNMP. Options are: • SNMPv2c: Allows SNMP service only to managers with SNMPv2c authentication. • SNMPv3: Allows SNMP service only to managers with SNMPv3 authentication. • SNMPv2c and SNMPv3: Allows SNMP service to managers with either SNMPv2c or SNMPv3 authentication. This is the default.	Format: Pulldown list Range: SNMPv2c, SNMPv3, or SNMPv2c and SNMPv3 Default: SNMPv2c and SNMPv3

Element	Description	Data Input Notes
Traps Enabled	Enables or disables SNMP trap output. The GUI user may selectively disable sending autonomous traps to SNMP managers when alarms are raised. Default is enabled. Access to alarm and KPI tables is not affected by this setting.	Format: Check box Range: Enabled or Disabled Default: Enabled
Traps from Individual Servers	Enables or disables SNMP traps from individual servers. If enabled, the traps are sent from individual servers, otherwise traps are sent from the Network OAM&P server.	Format: Check box Range: Enabled or Disabled Default: Disabled
SNMPV2c Read-Only Community Name	Configured Read-Only Community Name (SNMPv2c only). Public is the default. This field is required when SNMPv2c is enabled in Enabled Versions. The length of community name should be less than 32 characters.	Format: Alphanumeric [a-z, A-Z, 0-9] Range: 1 - 31 characters Default: snmppublic **Note:** The Community Name cannot equal "Public" or "Private".
SNMPV2c Read-Write Community Name	Configured Read-Write Community Name (SNMPv2c only). Public is the default. This field is required when SNMPv2c is enabled in Enabled Versions. The length of community name should be less than 32 characters.	Format: Alphanumeric [a-z, A-Z, 0-9] Range: 1 - 31 characters Default: snmppublic **Note:** The Community Name cannot equal "Public" or "Private".
SNMPv3 Engine ID	Configured Engine ID (SNMPv3 only). This field is required when SNMPv3 is enabled in **Enabled Versions**. A unique Engine ID value is generated by default.	Format: Hex digits 0-9 and a-f Range: 10 - 64 characters Default: A unique Engine ID value
SNMPv3 Username	Specifies an authentication username (SNMPv3 only). The default is TekSNMPUser. This field is required when SNMPv3 is enabled in Enabled Versions.	Format: Alphanumeric [a-z, A-Z, 0-9] Range: 1 - 32 characters Default: TekSNMPUser
SNMPv3 Security Level	Sets authentication and privacy options (used for SNMPv3 only).	Format: Pulldown list Range:

Element	Description	Data Input Notes
		• No Auth No Priv: Authenticate using the user name. No Privacy. • Auth No Priv: Authenticate using the MD5 or SHA1 protocol. No Privacy. • Auth Priv: Authenticate using the MD5 or SHA1 protocol. Encrypt using the AES or DES protocol. This is the default value. Default: Auth Priv
SNMPv3 Authentication Type	Sets authentication protocol (used for SNMPv3 only).	Format: Pulldown list Range: SHA-1 or MD5 Default: SHA-1
SNMPv3 Privacy Type	Sets privacy protocol (used for SNMPv3 only). This field is required when SNMPv3 Security Level is set to Auth Priv.	Format: Pulldown menu Range: • AES: Use Advanced Encryption Standard privacy. • DES: Use Data Encryption Standard privacy. Default: AES
SNMPv3 Password	Authentication password set up for the user specified in SNMPv3 Username (used for SNMPv3 only). This field is required when SNMPv3 is enabled and privacy is enabled in SNMPv3 Security Level.	Format: Any characters] Range: 8 - 64 characters

Adding a SNMP manager

Use this procedure to add a SNMP Manager:

1. Select **Administration > Remote Servers > SNMP Trapping**.

   The SNMP Trapping page appears.

2. Update **Enabled Versions** as appropriate.

   For more information about **Enabled Versions**, or any field on this page, see *SNMP administration elements* .

3. Select an empty **Manager** field and populate it with the hostname or IP address of the SNMP manager.

4. Enable traps from individual servers.
   This step is optional.
5. For SNMPv2c managers, optionally change the **SNMPV2c Read-Only Community Name**.
6. For SNMPv2c managers, optionally change the **SNMPV2c Read-Write Community Name**.
7. For SNMPv3 managers, choose an **SNMPv3 Security Level**, and optionally change the **SNMPv3 Engine ID, SNMPv3 Authentication Type**, and **SNMPv3 Privacy Type**.
8. For SNMPv3 managers with user authentication enabled, configure **SNMPv3 Username**.
9. For SNMPv3 managers with privacy enabled, configure **SNMPv3 Password**.
10. Click **OK** or **Apply** to submit the information.

The new manager and related settings are saved and activated.

Viewing SNMP trap settings

Use this procedure to view SNMP trap settings:

Select **Administration > Remote Servers > SNMP Trapping**.

The SNMP Trapping page appears. The page lists all SNMP options on the system.

Updating SNMP trap settings

Use this procedure to update SNMP trap settings:

1. Select **Administration > Remote Servers > SNMP Trapping**.

   The **SNMP Trapping** page appears.
2. Update SNMP trap settings as needed.
   For more information, see *SNMP administration elements* .
3. Click **OK** or **Apply** to submit the information.

The SNMP trap changes are saved and activated.

Deleting an SNMP trap managers

Use this procedure to remove one or more SNMP trap managers:

1. Select **Administration > Remote Servers > SNMP Trapping**.

   The **SNMP Trapping** page appears.
2. Delete the SNMP hostnames and IP addresses from the **Manager** fields for which you want traps removed.
3. Click **OK** or **Apply**.

The SNMP configuration changes are saved. If the SNMP manager hostnames and IP addresses are cleared from all Manager fields, the SNMP feature is effectively disabled.

Data Export

From the Data Export page you can set an export target to receive exported performance data. Several types of performance data can be filtered and exported using this feature. For more information about how to create data export tasks, see:

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting security log files*
- *Exporting KPIs*
- *Exporting measurements reports*

From the Data Export page you can manage file compression strategy and schedule the frequency with which data files are exported.

Data Export elements

This table describes the elements on the Data Export page.

Table 46: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server.	Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 255 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None
Username	Username used to access the export server	Format: Textbox Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9). To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None

Element	Description	Data Input Notes
Directory on Export Server	Directory path on the export server where the exported data files are to be transferred	Format: Textbox Range: Maximum length is 255 characters; valid value is any UNIX string. Default: None
Path to rsync on Export Server	Optional path to the rsync binary on the export server	Format: Textbox Range: Maximum length is 4096 characters; alphanumeric characters (a-z, A-Z, and 0-9),dash, underscore, period, and forward slash. Default: If no path is specified, the username's home directory on the export server is used
Backup File Copy Enabled	Enables or disables the transfer of the backup files.	Format: Checkbox Default: Disabled (unchecked)
File Compression	Compression algorithm used when exported data files are initially created on the local host.	Format: Radio button Range: gzip, bzip2, or none Default: gzip
Upload Frequency	Frequency at which the export occurs	Format: Radio button Range: fifteen minutes, hourly, daily or weekly Default: weekly
Minute	If The Upload Frequency is Hourly, this is the minute of each hour when the transfer is set to begin	Format: Scrolling list Range: 0 to 59 Default: zero
Time of Day	If the Upload Frequency is Daily of Weekly, this is the time of day the export occurs	Format: Time textbox Range: HH:MM AM/PM in 15-minute increments Default: 12:00 AM
Day of Week	If Upload Frequency is Weekly, this is the day of the week when exported data files will be transferred to the export server	Format: Radio button Range: Sunday through Saturday Default: Sunday
SSH Key Exchange	This button launches a dialog box. The dialog requests	Format: Button

Element	Description	Data Input Notes
	username and password and initiates SSH key exchange.	
Transfer Now	This button initiates an immediate attempt to transfer any data files in the export directory to the export server.	Format: Button

Configuring data export

The Data Export page enables you to configure a server to receive exported performance and configuration data. Use this procedure to configure data export.

1. Select **Administration > Remote Servers > Data Export**.
   The Data Export page appears.
2. Enter a **Hostname**.
   See the Data Export elements for details about the **Hostname** field and other fields that appear on this page.
3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. Enter the **Path to Rsync** on the Export server.
6. Select whether to enable the transfer of the backup file. To leave the backup disabled, do not check the box.
7. Select the **File Compression** type.
8. Select the **Upload Frequency**.
9. If you selected hourly for the upload frequency, select the **Minute** intervals.
10. If you selected daily or weekly for the upload frequency, select the **Time of Day**.
11. If you selected weekly for the upload frequency, select the **Day of the Week**.
12. Click **Exchange SSH Key** to transfer the SSH keys to the export server.
    A password dialog box appears.
13. Enter the password.
    The server will attempt to exchange keys with the specified export server. After the SSH keys are successfully exchanged, continue with the next step.
14. Click **OK** or **Apply**.
    The export server is now configured and available to receive performance and configuration data.

DNS Configuration

The following sections discuss the procedures used to set up the DNS (Domain Name System) configuration.

DNS configuration elements

The DNS Configuration page provides for configuration of the domain name system. This table describes the elements of the DNS Configuration page.

Table 47: DNS Configuration Elements

Element	Description	Data Input Notes
Domain	System Domain Name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Name Server 1	Address of a DNS name server	Format: Must be a valid ipv4 or ipv6 address
Name Server 2	Address of a DNS name server	Format: Must be a valid ipv4 or ipv6 address
Name Server 3	Address of a DNS name server	Format: Must be a valid ipv4 or ipv6 address
Search Domain 1	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Search Domain 2	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Search Domain 3	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Search Domain 4	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Search Domain 5	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters
Search Domain 6	A valid domain name	Format: alphanumeric, hyphen and decimal characters Range: Up to 255 characters

Adding a DNS Configuration

Use this procedure to add a DNS Configuration:

1. Select **Administration > Remote Servers > DNS Configuration**.

   The DNS Configuration page appears.

2. Enter the **Domain Name**.

3. Enter a **Name Server** for the external DNS name servers. You may enter up to three name servers.
4. Enter the **Search Domain** in the domain search order. You may add up to six search domain names.
5. Click **OK** or **Apply** to submit the information.

The new DNS configuration is saved and activated.

Updating a DNS Configuration

Use this procedure to update a DNS configuration:

1. Select **Administration > Remote Servers > DNS Configuration**.

   The DNS Configuration page appears.

2. Enter the updated **Domain** for the system.

   For more information about **Domain**, or any field on this page, see the DNS configuration elements.

3. Enter the updated name server in the appropriate fields. You may add up to three name servers.
4. Enter the updated search domain name in the appropriate fields. You may add up to six search domain names.
5. Click **OK** to submit the information.

The updated DNS configuration is saved and activated.

Chapter 4

Configuration

Topics:

This section describes configuration functions. Configuration data defines the network topology for the network. The topology determines the network configuration, the layout or shape of the network elements, and their components. It defines the interlinking and the intercommunicating of the components. The network topology represents all server relationships within the application. The server relationships are then used by MiddleWare to control data replication and data collection, and define HA relationships.

Network Elements

This application is a collection of servers linked by standardized interfaces. Each server can be used multiple times in a network for load balancing or organizational issues. Network Elements are containers that group and create relationships among servers in the network. These relationships allow the software and hardware to properly work together. Understanding the relationships among the servers allows you to configure the system. The primary network element relationship is the network element to server. Servers are assigned to network elements. A network element can contain multiple servers but a single server is part of only one network element. The attributes of a server include the network element to which it belongs.

Configuration of Network Elements must follow a specific chronology.

1. Configure the first Network Element, beginning with the configuration of switches. After the switches are configured, the first NOAMP server must be configured through the GUI interface.
2. After the first NOAMP server has been configured, configure the second NOAMP.
3. If the system supports SOAMs, and after the first Network Element is configured and running, additional Network Elements can be configured to support SOAM servers.

Network Elements Insert elements

These tables describe the elements of the **Network Elements Insert** page.

Note: Networks are no longer configured using the Network Element pages. Networks can still be added when uploading an XML file to configure a network element. To complete network configuration, see the Networks section.

Note: A signaling network element can only be added after a NOAMP with at least one server has been added.

Element	Description	Data Input Notes
Network Element Name	The user-defined name for the network element.	Format: 1 to 32-character string that must contain at least one alphabetic character and must not start with a digit Range: alphanumeric characters and underscore

Inserting a network element

You define a network by configuring network elements and adding servers to the network elements. A maximum of sixteen (16) network elements can be configured.

Note: Network information is no longer configured using the Network Element pages. To complete network configuration, see the Networks section.

Use this procedure to configure and insert a network element:

1. Select **Configuration > Network Elements**.

The **Network Elements** page appears.

2. Click **Insert**.

   The **Network Elements Insert** page appears.

3. Enter a unique name across the network element table in **Network Element Name**.

   See *Network Elements Insert elements* for details about the **Network Element Name** field and other fields that appear on this page.

4. Click **OK** to submit the information and return to the **Network Elements** page.

The network element is added to the topology database tables, and the GUI displays the updated Network Elements table.

Uploading a configuration file

Use this procedure to upload an XML file to configure a new network element:

1. Select **Configuration > Network Elements**.

   The **Network Elements** page appears.

2. Click **Choose File** to locate the file you want to use to configure a new network element.

   The **File Upload** window appears.

3. Select the file you want to use to configure a new network element.

   The selected file appears in the text box.

4. Click **Upload File**.

Data validation is performed immediately. If the file is valid, a new network element is created. Alternately, a file that contains invalid parameters returns an error message, and no network element is created.

Viewing Network Elements

Use this procedure to view network elements:

1. Select **Configuration > Network Elements**.
   The **Network Elements Configuration** page appears.
2. Click on the folder icon beside the **Network Element Name** to view additional information about the selected network element.

Deleting a Network Element

Before a network element can be deleted there must be no servers associated with the network element.

Use this procedure to delete a network element:

1. Select **Configuration > Network Elements**.

   The **Network Elements** page appears.

2. Click to select the network element you want to delete and click **Delete**.

   A delete confirmation message appears.

3. Click **OK** to delete the network element from the database tables.
   The updated **Network Elements Configuration** page appears.

The network element is deleted from the topology databases.

Network Element Report Elements

The report is divided into three sections, and each section contains subsections. Any field for which there is no data will display the value "n/a".

Table 48: Layer-3 Network Element Report

Section	Subsection
Network Element Summary	Each network element is listed individually with related general information. • RSTP Enabled • Frame ID • Position • Demarcation Type • Commit State
Network Report	Each network element is listed individually with information about network. • Network Name: Name for the network • VLAN ID: Three character numeric VLAN ID • Network ID: Numeric network ID • Netmask: Mask used to divide an IP address into subnets and specify the networks available hosts • Gateway: IP address for Gateway server • Type: Network type • Default: Whether the network is the default gateway
Server Report	Each network element is listed individually with information about the related servers. • Hostname: name of server associated with the network element • XMI Address: XMI address for server • IMI Address: IMI address for server • RMM Address: n/a

Generating a Network Element Report

A network element report provides a summary of the network element configuration. This report can be used to:

- View network element configurations
- Compare network element configurations to system manager network configurations
- Relate network elements to servers, VLANs, and systems
- View a list of the locations the application occupies
- View a list of the IP addresses in the application topology

This report can also be printed or saved to a file.

Use this procedure to generate a network element report:

1. Select **Configuration > Network Elements**.

   The **Network Elements** page appears.

2. To generate a report for a single network element, click to select the network element and click **Report**. To generate a report for all configured network elements, click **Report**.

   Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

   The Network Element Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Exporting a network element

The network element export button generates an installation script file used for hardware configuration. Use this procedure to export the configuration parameters of a network element:

1. Select **Configuration > Network Elements**.

   The **Network Elements** page appears.

2. Click to select a network element from the table.
3. Click **Export**.
   A CSV file is created.

Network

The Network pages allow the user to configure signaling networks, devices, and routes. Through the Network Configuration page, network IDs and subnets can be added to enable servers to communicate with the signaling networks. Route configuration allows the user to define specific routes for signaling traffic. Device configuration allows the user to configure additional interfaces on MP servers used in signaling networks.

Network Insert elements

This table describes the elements of the Network Insert page.

Table 49: Network Insert Elements

Field	Description	Data Input Notes
Network Name	The name of the Network	Format: Alphanumeric; must begin with a letter Range: 31 character maximum
Network Element	The network element associated with the network. If not specified, the network will be available to servers in all network elements.	Format: Drop down list
VLAN ID	The VLAN ID of the Network	Format: Numeric Range: 1-4094 **Note:** VLAN IDs 1-4 are reserved for Management. VLAN IDs that are already in use cannot be reused.
Network Address	The network address of the Network	Format: Valid network address Range: Dotted decimal (IPv4) or colon hex (IPv6)
Netmask	Subnetting to apply to servers within the Network	Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4)
Router IP	The IP address of a router on this network. **Note:** If this is a default network, this will be used as the gateway address of the default route on servers with interfaces on this network. If customer router monitoring is enabled, this address will be the one monitored.	Format: Valid IP address
Default Network	Whether the network is the default gateway	Format: Radio button Range: Yes or No

Field	Description	Data Input Notes
Routable	Whether the network is routable outside its network element. **Note:** If it is not assigned to a network element, it is assumed to be possibly present in all network elements.	Format: Radio button Range: Yes or No

Inserting a Network

Use the following procedure for inserting a network. Alternatively, you can also use the procedures included in the Network Elements topics.

1. Select **Configuration > Network**
   The **Network** page appears.
2. Click the **Insert** button.
   The **Network Insert** page appears.
3. Enter a **Network Name**.
   For more information about **Network Name**, or any field on this page, see *Network Insert elements* .
4. Enter a **VLAN ID**.
5. Enter a **Network Address**.
6. Enter a **Netmask**.
7. Click **OK** to submit the information and return to the Network page, or click **Apply** to submit the information and continue entering additional data.

The new network is added.

Configuration Network elements

This table describes the elements of the **Configuration Network** page.

Table 50: Configuration Network Elements

Field	Description
Network Name	The name associated with the network
VLAN	VLAN ID associated with the network
Network	The IP address associated with the network in the format: IP Address/Prefix Length

Editing a Network

Not all networks can be edited. Pre-configured networks created during the install process, for example, cannot be edited. A network that cannot be edited is distinguished using italic font.

Note: Prior to editing a network, generate a network report. The network report will serve as a record of the network's original settings. Print or save the network report for your records. For more information about generating a network report, see *Generating a Network Report*.

1. Select **Configuration > Network**
   The **Network** page appears.
2. Click to select a network and click **Edit.**

   Note: If the network is currently unlocked, the button will read **Lock**. If the button is currently locked, the button will read **Unlock**.

   If the network can be edited, the **Network Edit** page appears.
3. Edit the available fields as necessary.
   See *Network Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.
4. Click **OK** to submit the changes and return to the **Network** page, or click **Apply** to submit the information and continue editing additional data.

The network is changed.

Locking and Unlocking a Network

Any network on the system can be locked or unlocked. When a network is locked, no modifications may be made to any device or route that uses that network. To add route or a device to a network, the network would have to be in an unlocked state.

1. Select **Configuration > Network**
   The **Network** page appears.
2. Click to select a network and click **Lock/Unlock.**

   Note: If the network is currently unlocked, the button will read **Lock**. If the button is currently locked, the button will read **Unlock**.
3. At the confirmation window, click **OK**. When unlocking a network, you will also have to confirm your decision using a check box.

The network is locked or unlocked.

Deleting a Network

Not all networks can be deleted. In-use networks and pre-configured networks created during the install process, for example, cannot be deleted. A network that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a network, generate a network report. The network report will serve as a record of the network's original settings. Print or save the network report for your records. For more information about generating a network report, see *Generating a Network Report*.

1. Select **Configuration > Network.**
   The **Network** page appears.
2. Click to select the network you want to delete. Alternately, you can delete multiple networks. To delete multiple networks, press and hold **Ctrl** and click to select specific networks.

Note: If the network cannot be deleted, the **Delete** button will be disabled.

Note: To delete multiple networks at one time, all selected networks must be deletable.

3. Click **Delete**.
   A confirmation box appears.
4. Click **OK** to delete the network.
   The network is deleted.

Generating a Network Report

A network report provides a summary of the configuration of one or more networks. Reports can be printed or saved to a file.

1. Select **Configuration > Network**
   The **Network** page appears.
2. Click **Report** to generate a report for all networks. To generate a report for a single network, click to select the network and click **Report**. Alternately, you can select multiple networks. To generate a report for multiple networks, press and hold **Ctrl** as you click to select specific networks.
   The Network Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Devices

Device configuration allows the user to configure interfaces on MP servers used in signaling networks.

Device Insert elements

This table describes the elements of the Devices Insert page.

Table 51: Devices General Options

Field	Description	Data Input Notes
Device Type	The type of device	Format: Radio button Range: Ethernet, Bonding, VLAN, Alias **Note:** Ethernet is not selectable.
Device Monitoring	The monitoring style to use with a bonding device	Format: Pulldown list Default: MII Range: MII, ARP **Note:** Device Monitoring is disabled

Field	Description	Data Input Notes
		when the Device Type is not Bonding.
Start on Boot	When selected, this checkbox enables the device to start on boot.	Format: Checkbox Default: Enabled
Boot Protocol	The boot protocol	Format: Pulldown list Range: None, DHCP Default: None
Base Device(s)	The base device(s) for Bond, Alias, and VLAN device types **Note:** Alias and VLAN devices require one selection; bond devices require two selections.	Format: Checkbox Range: Available base devices

The **MII Monitoring Options** and **ARP Monitoring Options** tabs collect settings for MII and ARP monitoring, respectively. The **IP Interfaces** tab allows interfaces to be associated with a device.

Table 52: Devices MII Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: None and available devices Default: None
Monitoring Interval	MII monitoring interval in milliseconds	Range: A positive integer Default: 100ms
Upstream Delay	MII monitoring upstream delay in milliseconds	Range: A positive integer Default: 200ms
Downstream Delay	MII monitoring downstream delay in milliseconds	Range: A positive integer Default: 200ms

Table 53: Devices ARP Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: Available devices
Monitoring Interval	ARP monitoring interval in milliseconds	Range: A positive integer Default: 100ms

Field	Description	Data Input Notes
ARP Validation	The method to validate the ARP probes and replies	Format: Pulldown list Range: None, Active, Backup, All Default: None
ARP Target IP(s)	Comma-separated ARP target IP addresses	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Table 54: Devices IP Interfaces tab

Field	Description	Data Input Notes
IP Address List	The IP address of the interfaces associated with the device	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Add Row	Displays a textbox to add an IP Address	Format: Button **Note:** Multiple rows can be added.
IP Address textbox	Textbox for an IP address	Format: Textbox Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Remove	Removes the device interface IP Address on the selected row	Format: Button

Inserting a Device

Devices cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.
2. Select a server.
3. Click the **Insert** button.
   The **Device Insert** page appears.
4. Select a **Device Type**.

   For more information about **Device Type**, or any field on this page, see *Device Insert elements* .

   Note: Device Type of Ethernet cannot be selected.

5. Select a **Device Monitoring** style.

   Note: Device Monitoring is only used when the Device Type is Bonding.

6. By default, **Start on Boot** is enabled. Uncheck the check box if you want to disable **Start on Boot**.
7. Select the **Boot Protocol**.
8. Select the **Base Device(s)** if the device type is one of the following: Bond, Alias, or VLAN.

   Note: Alias and VLAN devices require one selection; bond devices require two selections.

9. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The device is added. You can now update MII and ARP monitoring options and add IP interfaces, if applicable.

Inserting MII Monitoring Options

Inserting MII monitoring options is only required if the device type is Bonding. For all other device types, the **MII Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.
2. Select a server.
3. Click the **Insert** button.
   The **Device Insert** page appears.
4. Click the **MII Monitoring Options** tab.
   The **MII Monitoring Options** tab appears.
5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.
6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.
7. Enter the **Upstream Delay**, if you do not wish to use the default setting.
8. Enter the **Downstream Delay**, if you do not wish to use the default setting.
9. Click the **General Options** tab.
10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The MII monitoring options are updated.

Inserting ARP Monitoring Options

Inserting ARP monitoring options is only required if the device type is Bonding. For all other device types, the **ARP Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.
2. Select a server.
3. Click the **Insert** button.
   The **Device Insert** page appears.
4. Click the **ARP Monitoring Options** tab.
   The **ARP Monitoring Options** tab appears.
5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.
6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.
7. Click **ARP Validation** to select a validation method from the pulldown list, if you do not wish to use the default setting.

8. Enter one or more IP addresses for the target device.

   Note: Multiple IP addresses are comma separated.

9. Enter an IP Address for the device.
10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The ARP monitoring options are updated.

Inserting IP Interfaces

The IP interfaces tab allows interfaces to be associated with a device.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.
2. Select a server.
3. Click the **Insert** button.
   The **Device Insert** page appears.
4. Click the **IP Interfaces** tab.
   The **IP Interfaces** tab appears.
5. Click **Add Row**.
   A textbox appears in which you can enter an IP Address for the device.
6. Enter an **IP Address** for the device.
7. Select a **Network Name**.
8. For each row, only one IP Address and Network Name can be specified. To specify additional rows, select **Add Row** and following Steps 6 and 7.
9. When you are finished adding IP Addresses, click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The IP addresses are added.

Devices elements

This table describes the elements of the **Configuration Devices** page.

Table 55: Devices Elements

Field	Description
Server	The server host name displayed in tabbed format at the top of the table
Device Name	The name of the device
Device Type	The device type. Supported types include: • Bonding • VLAN • Alias • Ethernet
Device Options	A collection of keyword value pairs for the device options

Field	Description
IP Interface (Network)	IP address and network name in the format: IP Address (network name)
Configuration Status	The configuration status of the device. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Device

Not all devices can be edited. Pre-configured devices created during the install process, for example, cannot be edited. A device that cannot be edited is distinguished using italic font.

Note: Prior to editing a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. Click to select a device and click **Edit.**

   Note: If the device cannot be edited, the **Edit** button will be disabled.

   If the device can be edited, the **Device Edit** page appears.
4. Edit the available fields as necessary.
   See *Device Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.
5. Click **OK** to submit the changes and return to the **Devices** page, or click **Apply** to submit the information and continue editing additional data.

The device is changed.

Deleting a Device

Not all devices can be deleted. In-use devices and pre-configured devices created during the install process, for example, cannot be deleted. A device that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices.**

The **Devices** page appears.

2. Click to select a server.
   The device data for the selected server appears.
3. Click to select the device you want to delete. Alternately, you can delete multiple devices. To delete multiple devices, press and hold **Ctrl** and click to select specific devices.

   Note: If the device cannot be deleted, the **Delete** button will be disabled.

   Note: To delete multiple devices at one time, all selected devices must be deletable.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK**.
   The device is deleted.

Generating a Device Report

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. To generate a report for all devices, click **Report**. To generate a report for a single device, click to select the device and click **Report**. Alternately, you can select multiple devices. To generate a report for multiple devices, press and hold **Ctrl** as you click to select specific devices.
   The Device Report is generated.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Routes

Use the Route Configuration page to define specific routes for signaling traffic. You can specify routes for the entire network, specific servers, or specific server groups.

Routes Insert elements

This table describes the elements of the Routes Insert page. Elements are displayed for the selected server or server group.

Table 56: Routes Insert Elements

Field	Description	Data Input Notes
Route Type	The type of route	Format: Radio button Range: Default, Net, Host **Note:** The Default route option is available only if there is no default

Field	Description	Data Input Notes
		route configured on the target server. There can be no more than one IPv4 and one IPv6 default route defined.
Device	The network device name through which traffic is routed	Format: Pulldown list Range: Provisioned devices on the selected server
Destination	The destination network address **Note:** This field is disabled if the **Route Type** is default.	Format: Valid network address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Netmask	A valid netmask for the destination network **Note:** This field is disabled if the **Route Type** is default. This field is disabled and set to 32 (IPv4) or 128 (IPv6) if the **Route Type** is host.	Format: Valid netmask Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4) Default: 24 for IPv4; 64 for IPv6
Gateway IP	The IP Address of the gateway for the route	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Inserting a Route

Routes cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Routes**
   The **Routes** page appears.
2. Using the tabs, select to add a server or server group to the entire network, or a specific network group.
3. Click the **Insert** button.
   The **Routes Insert** page appears.
4. Select a **Route Type**.

   For more information about **Route Type**, or any field on this page, see *Routes Insert elements* .

5. Select a **Device**.
6. Enter a **Destination**.

   Note: This step is required only if the **Route Type** is Net or Host. The field is disabled if the **Route Type** is Default.

7. Enter the **Netmask**.

   Note: This step is required only if the **Route Type** is Net. The field is disabled if the **Route Type** is Default or Host.

8. Enter the **Gateway IP**.
9. Click **OK** to submit the information and return to the Route page, or click **Apply** to submit the information and continue entering additional data.

The route is added.

Routes elements

This table describes the elements of the **Configuration Routes** page.

Table 57: Routes Elements

Field	Description
Server/Server Group	The server host name and server groups are displayed in tabbed format at the top of the table
Route Type	The type of route
Destination	The destination network IP address and prefix length in the format: IP Address/Prefix Length
Netmask	A valid netmask for the destination network
Gateway	The IP Address of the gateway for the route
Scope Status	The current number of servers where the route was successfully configured out of the total servers in the server group. (Note: This column is only present for server group routes)
Configuration Status	The configuration status of the route. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Route

Not all routes can be edited. Pre-configured routes created during the install process, for example, cannot be edited. A route that cannot be edited is distinguished using italic font.

Note: Prior to editing a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes**.
   The **Routes** page appears.
2. Click to select a server or server group using the tabs at the top of the table.
   The route data for the selected server or server group appears.
3. Click to select a route and click **Edit.**

   Note: If the route cannot be edited, the **Edit** button will be disabled.

   If the route can be edited, the **Routes Edit** page appears.
4. Edit the available fields as necessary.
   See *Routes Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.

5. Click **OK** to submit the changes and return to the **Routes** page, or click **Apply** to submit the information and continue editing additional data.

The route is changed.

Deleting a Route

Not all routes can be deleted. In-use routes and pre-configured routes created during the install process, for example, cannot be deleted. A route that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes.**
   The **Routes** page appears.
2. Click to select a server or server group from the tabs at the top of the table.
   The route data for the selected server or server group appears.
3. Click to select the route you want to delete. Alternately, you can delete multiple routes. To delete multiple routes, press and hold **Ctrl** and click to select specific routes.

   Note: If the route cannot be deleted, the **Delete** button will be disabled.

   Note: To delete multiple routes at one time, all selected routes must be deletable.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK** to delete the route
   The route is deleted.

Generating a Route Report

1. Select **Configuration > Network > Routes**
   The **Routes** page appears.
2. Click to select a server or server group from the tabs at the top of the table.
3. Click **Report** to generate a report for all routes. To generate a report for a single route, click to select the route and click **Report**. Alternately, you can select multiple routes. To generate a report for multiple routes, press and hold **Ctrl** as you click to select specific routes.
   The Route Report is generated.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Services

This application allows for flexible network deployment, with each installation being able to configure network elements with one or more networks and map a specific service to those networks. This flexibility allows for individual configuration of network routes. The system only defines the default route if the default network is defined for the network element.

Configuration of services must follow a specific chronology.

1. Configure the first NOAMP Network Element And Server.
2. Use the Services screen to map networks to services.

   Note: It is important that Services be configured after the insertion of the NOAMP NE and before configuring any servers.

3. Configure the first NOAMP server.
4. Configure the NOAMP server group.
5. Add the first NOAMP server to the group.
6. Configure the second NOAMP server.
7. Add the second NOAMP server to the group.
8. Configure the SOAM NE.
9. Configure the SOAM servers.
10. Configure the SOAM server group.
11. Add the SOAM servers to the group.
12. Configure any MP servers.
13. Add MP servers into server groups, as necessary.

Editing Service information

Services are set during installation of the system. However, you can edit network characteristics of the services. Use this procedure to edit existing service information:

1. Select **Configuration > Services**.

   The Services page appears.

2. Click **Edit**.

   The Services [Edit] page appears.

3. Select from the available choices to determine the Intra-NE Network.
4. Select from the available choices to determine the Inter-NE Network.
5. Select **Apply** to save the changes you have made and remain on this screen, or select **OK** to save the changes and return to the Services page.

Generating a Service Report

A service report provides a summary of the service configuration. This report can also be printed or saved to a file.

Use this procedure to generate a service report:

1. Select **Configuration > Services**.

   The Services page appears.

2. Click **Report**.
   The Services Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.
5. Click **Back** to return to the Services page.

Servers

Servers are the processing units of the application. Servers perform various roles within the application. The roles are:

- Network OAMP (NOAMP) - The NOAMP is one active and one standby server running the NOAMP application and operating in a high availability global configuration. It also provides a GUI which is used for configuration, user administration and the viewing of alarms and measurements.
- System OAM (SOAM) - The SOAM is the combination of an active and a standby application server running the SOAM application and operating in a high availability configuration. SOAM also provides a GUI used for local configuration and viewing alarms and measurements details specific to components located within the frame (SOAM, MP). The SOAM supports up to 8 MPs.

  Note: SOAM is not an available role in systems that do not support SOAMs.

- MP - MPs are servers with the application installed and are configured for MP functionality.
- Query Server (QS) - The Query Server is an independent application server containing replicated application data. A Query Server is located in the same physical frame as each NOAMP component.

The role you define for a server affects the methods it uses to communicate with other servers in the network. For more information about how each interface is used, refer to the Network Installation Guide that came with the product.

Add new server configuration elements

This table describes the elements on the **Adding a new server** page:

Table 58: Add New Server Configuration Elements

Element	Description	Data Input Notes
Hostname	The defined name for the server. The name must be unique across the server table. Alphanumeric (A-Z, a-z, 0-9) and hyphen (-) characters are allowed. The Hostname must begin and end with an alphanumeric character.	Format: Alphanumeric (A-Z, a-z, 0-9) and hyphen (-) characters. Hostname must begin and end with an alphanumeric character. Range: Maximum length is 20 characters
Role	The defined type for the network element The Role selected here affects which of the following IP Addresses are available to be configured.	Format: Pulldown list Range: Network OAM&P, System OAM, MP, Query Server **Note:** System OAM is not an available role in systems that do not support SOAMs.
System ID	System ID for the NOAMP or SOAM server.	Default = none Range = A 64-character string. Valid value is any text string.
Hardware Profile	The hardware profile of the server	Format: Pulldown list of customized options
Network Element Name	The network element must first be set up using the **Configuration > Network Elements** page.	Format: Pulldown list Range: A valid Network Element
Location	Optional, user supplied field to identify the location of the server.	Format: Text string Range: Maximum length is 15 characters
Interfaces: Network	The list of available interfaces from the hardware profile.	Format: n/a
Interfaces: IP Address	The IP address of the network	Format: numeric
Interfaces: Interface	The interface with which the IP address is associated. The list is populated with the available interfaces from the hardware profile.	Format: drop down list

Element	Description	Data Input Notes
	Typically, this list includes bond interfaces (e.g., bond0 and/or bond1). One interface is displayed for each network in the network element.	
Interfaces: VLAN	This checkbox allows the user to decide whether to create a VLAN interface. If the box is checked, a VLAN interface will automatically be created. If the box is not checked, the IP address will be assigned directly to the interface selected from the dropdown box. Only one IP address can be associated with a non-VLAN interface (e.g., bond1). One checkbox is displayed for each interface.	Format: checkbox
Interfaces: Prefer	Selection of preferred NTP sources, multiple sources can be designated as preferred. Every NTP Server IP Address field has a corresponding "Prefer" checkbox.	Format: checkbox
Interfaces: NTP Server IP Address	The IP address of the NTP Server	Format: numeric

Inserting a Server

Servers can be inserted only after a network element has been provisioned.

Use this procedure to insert a server:

1. Select **Configuration > Servers**.
2. Click **Insert** at the bottom of the table.

   The **Adding a new server** page appears.

3. Enter a **Hostname.** This is a user-defined name for the server. The server name must be unique across the server table.

   For more information about **Hostname**, or any field on this page, see *Add new server configuration elements* .

4. Select a **Role**.
5. Enter the **System ID**.

6. Select a **Hardware Profile**.
7. Select a **Network Element Name**.

   Select from the network element names defined previously on the Network Element Configuration page.
8. Enter the **IP address** for the appropriate network in the Interfaces grid
9. Select the **Interface** in the Interfaces grid.
10. Select the **VLAN ID** for the network in the Interfaces grid, if applicable.
11. Select the **Prefer** checkbox for preferred sources.
12. Select **Add** to add the NTP Server IP Address. Enter the NTP Server IP Address in the text box.
13. Enter the **NTP Server IP Address** in the text box.
14. Select the **Prefer** checkbox for the NTP Server IP Addresses.
15. Enter a **Location**.
16. Click **OK** to submit the information and return to the Servers Configuration page, or click **Apply** to submit the information and continue entering additional data.

The server is added to the network databases.

Servers Configuration elements

The **Servers Configuration** page lists all servers that are provisioned. This table describes the elements of the **Servers Configuration** page.

Element	Description
Hostname	The defined name for the server. The name must be unique across the server table. Alphanumeric (A-Z, a-z, 0-9) and hyphen (-) characters are allowed. The Hostname must begin and end with an alphanumeric character.
Role	The defined role for the network element. Types are: • Network OAMP - A pair of servers implementing OAMP functions for the entire network. There is only one pair of NOAMP Servers per network, and they comprise the NOAMP Network Element. There can be only two servers of this type in the Servers table. • System OAM - Pairs of servers implementing a centralized database and local OAM functions for each SO Network Element deployed. There can be only two servers of this type per signaling Network Element. **Note:** System OAM is not an available role in systems that do not support SOAMs. • MP - Each pair or cluster of servers implementing message processing functions.

Element	Description
	• Query Server - An independent application server that contains a replicated version of the PDBI database. It accepts replicated subscriber data from the NOAMP and stores it in a customer accessible database. The Role selected here affects which of the following IP Addresses and VLAN IDs are available to be set up.
System ID	The system ID
Server Group	The server groups to which the server belongs.
Network Element	The name of the network element that is associated with each server. The network element must first be configured using the **Configuration > Network Elements** page before it can be associated with a server.
Location	The location of the server. This field is optional.
Place	The Place that the server is assigned to.
Details	Lists provisioned IP addresses.

Viewing Servers

Use this procedure to view servers:

Select **Configuration > Servers**.

The Servers Configuration page appears.

Deleting a Server

Before a server can be deleted the following conditions must be true:

- The server is not part of a server group.
- The server is not configured as a server pair.

Use this procedure to delete a server:

1. Select **Configuration > Servers**.

   The **Servers Configuration** page appears.

2. Click to select the server you want to delete.
3. Click **Delete**.

   Click **Yes** to confirm.

The server is deleted from the network database table.

Exporting a server

The server export button generates an installation script file used for hardware configuration. Use this procedure to export a single server. For information about how to export multiple servers at once, see *Exporting multiple servers*.

1. Select **Configuration > Servers**.
2. Click to select a server to export.
3. Click **Export**.

   The server data is exported to an SH file.
4. Click Info.

   The **Info** box appears.
5. Click the **download** link to download the file.

Exporting multiple servers

The server export button generates an installation script file used for hardware configuration. Use this procedure to export more than one server.

1. Select **Configuration > Servers**.
2. Press and hold **Ctrl** as you click to select multiple servers.
3. Click **Export**.

   Data for the selected servers is exported to individual SH files located on the **Status and Manage > Files** page.
4. Click **Info.**

   The **Info** box appears.
5. Click the **Status and Manage > Files** link.
   The **Status and Manage > Files** page appears. The SH files for the server data exported in this procedure is located on the **Status and Manage > Files** page.

Generating a Server Report

Use this procedure to generate a server report:

1. Select **Configuration > Servers**.
2. Click to select the server for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.
3. Click **Report**.
   The servers report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Server Groups

The Server Groups feature allows the user to assign a function, parent relationships, and levels to a group of servers that share the same role, such as OAMP, SOAM, and MP servers. The Server Groups feature also enables users to create new groups, add servers to existing groups, edit groups, delete servers and server groups, and generate reports that contain server group data.

The Server Group parent selection can now be modified for C-Level servers, dependent upon application allowing the change.

Server Groups Insert elements

This table describes the elements of the **Insert Server Groups** page.

Element	Description	Data Input Notes
Server Group Name	A unique name used to label the server group.	Format: Alphanumeric characters and underscore "_" are allowed. A minimum of one alphabetic character is required. **Note:** Server Group Name must not start with a digit. Range: Maximum length is 32 characters.
Level	The level of the servers belonging to this group.	Format: Pulldown menu Range: Levels A, B, or C
Parent	The parent server group that functions as the replication parent of the selected server group	Format: Pulldown menu **Note:** If the level of the group being inserted is A, then the parent field is not editable and NONE is displayed in the pulldown menu.
Function	The defined function for the server group.	Format: Pulldown menu Range: Functions supported by the system
WAN Replication Connection Count	Specify the number of TCP connections that will be used by replication over any WAN connection associated with this Server Group.	Range = An integer between 1 and 8 Default = 1

Inserting a Server Group

Use this procedure to configure a server group:

1. Select **Configuration > Server Groups**.
2. Click **Insert**.

   The **Insert Server Groups** page appears.

3. Enter the **Server Group Name.**

   For more information about **Server Group Name**, or any of the fields on this page, see *Server Groups Insert elements*.

4. Select a **Level** from the pulldown menu.
5. Select a **Parent** from the pulldown menu.
6. Select a **Function** from the pulldown menu.
7. Enter a **WAN Replication Connection Count.**
8. Click **OK** to submit the information and return to the Server Groups page, or click **Apply** to submit the information and continue adding additional data.

Server Groups configuration elements

The **Server Groups Configuration** screen lists all server groups. The following information is displayed.

Element	Description
Server Group Name	A unique name used to label the server group. Alphanumeric characters and '_' are allowed. A minimum of one alphabetic character is required. The name cannot start with a digit. Maximum length is 32 characters.
Level	The level of the servers belonging to this group.
Parent	The parent server group that functions as the replication parent of the selected server group.
Function	The defined function for the server group.
Connection Count	The number of TCP connections that will be used by replication over any WAN connection associated with this Server Group.
Servers	The list of servers in the server group.

Server Groups Edit elements

The **Edit Server Groups** page allows you to edit existing server groups. This table describes the elements of the **Edit Server Groups** page.

Element	Description	Data Input Notes
Server Group Name	A unique name used to label the server group.	Format: Alphanumeric characters and underscore "_" are allowed. A minimum of one alphabetic character is required. Must begin with an alphabetic character. Range: Maximum length is 32 characters.
Function	The defined function for the server group.	This field cannot be edited.
WAN Replication Connection Count	The number of TCP connections that will be used by replication over any WAN connection associated with this Server Group.	Range = An integer between 1 and 8 Default = 1
Server	IP Address of the server to be used for clock synchronization. This field is optional.	Format: Valid IP address, or field may be left blank Range: Dotted quad decimal (IPv4) or colon hex (IPv6) **Note:** Server is editable for A-Level server groups. C-Level server groups are editable if allowed by the application.
SG Inclusion	When checked, the server is included in the server group.	Checkbox
Preferred HA Role	When checked, the server is marked as a preferred spare. When marked as a preferred spare, the server only assumes an active or standby role if all the other servers in the server group are unavailable.	Checkbox
VIP Assignment: VIP Address	A virtual IP address shared by the servers in this group that have networking interfaces on the same layer-2 network.	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Editing a Server Group

Once a server group is created, certain values can be edited, and available servers can be added to or deleted from the server group. Use this procedure to edit a server group:

1. Select **Configuration > Server Groups**.
2. From the table, click to select the server group you want to edit.
3. Click **Edit**.
   The **Edit Server Groups** page appears.
4. Edit the values you want to change.
   Fields that cannot be edited will be grayed out. For more information about these fields, or any of the fields in this procedure, see *Server Groups Edit elements*.
5. Click **OK** to submit the information and return to the **Server Groups** page, or click **Apply** to submit the information and continue adding additional data.

Adding a server to a server group

Once a server group is created, servers can be added. Use this procedure to add a server to a server group:

1. Select **Configuration > Server Groups**.
2. From the table, click to select the server group you want to edit.
3. Click **Edit**.
   The **Edit Server Groups** page appears. The Edit Server Groups page displays the servers in the network element that are possible candidates for inclusion in the server group.
4. To add a server to the server group, select the checkbox for **SG Inclusion**. When checked, the server will be included in the server group.
5. To add a virtual IP address, select **Add** in the **VIP Assignment** section and enter the virtual IP address.
6. Click **OK** to submit the information and return to the **Server Groups** page, or click **Apply** to submit the information and continue adding additional data.

Deleting a server from a server group

Use this procedure to delete a server from a server group:

1. Select **Configuration > Server Groups**.
2. From the table, click to select the server group you want to edit.
3. Click **Edit**.
   The **Edit Server Groups** page appears.
4. To delete a server from the server group, select the checkbox for **SG Inclusion**. When checked, the server will be included in the server group.
5. Click **OK** to submit the information and return to the **Server Groups** page.

Assigning a VIP to a server group

Use this procedure to assign a VIP to a server group.

Note: This procedure is optional and is only supported if the system supports VIP.

1. Select **Configuration > Server Groups**.
2. From the table, click to select the server group you want to edit.
3. Click **Edit**.
   The **Edit Server Groups** page appears.
4. Click **Add** to add a new VIP address to the server group.

   Note: Multiple VIP addresses can be added.

5. Insert the **VIP address**.
6. Click **OK** to submit the information and return to the **Server Groups** page, or click **Apply** to submit the information and continue adding additional data.

Removing a VIP from a server group

Use this procedure to remove a VIP address from a server group:

1. Select **Configuration > Server Groups**.
2. From the table, click to select the server group you want to edit.
3. Click **Edit**.
   The **Edit Server Groups** page appears.
4. Click to select the VIP you want to remove from the server group.
5. Click **Remove**.

   The VIP address is removed from the server group.

6. Click **OK** to submit the information and return to the **Server Groups** page, or click **Apply** to submit the information and continue adding additional data.

Deleting a Server Group

Use this procedure to delete a server group.

Note: Only a server group with no existing servers in the group can be deleted. For information about how to delete a server from a server group, see *Deleting a Server*.

1. Select **Configuration > Server Groups**.
2. Click to select the server group you want to delete from the table.
3. Click **Delete**.

   A delete confirmation message appears in a pop up window.

4. Click **OK** to delete the server group.

   If you click **Cancel**, the server group will not be deleted, and you will be returned to the Server Groups page.

Server Group Report Elements

The report is divided into two sections and each section contains subsections.

Note: Fields with no data display "n/a" with the exception of Virtual IP Address(es) and NTP Server(s). Virtual IP Address(es) and NTP Servers(s) fields are optional. If no data exists for those fields, then the fields will not display in the report.

Section	Subsection
Server Groups Summary	Each server group is listed individually with related general information. For details about these values, see *Server Groups Edit elements*. • Name • Level • Connection Count • Parent • Function • Server(s) • Virtual IP Address(es)
Server Report	Each network element is listed individually with information about the related servers.

Generating a Server Group Report

Use this procedure to generate a server group report:

1. Select **Configuration > Server Groups**.
2. Click to select the server group for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.
   The server group report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Resource Domains

The Resource Domains function allows you to assign servers to domains.

Add new resource domain elements

This table describes the elements for adding a resource domain element:

Table 59: Add New Resource Domain Elements

Element	Description	Data Input Notes
Resource Domain Name	The name for the resource domain.	Format: Alphanumeric (A-Z, a-z, 0-9) and underscore (_) characters. Range: Maximum length is 32 characters
Resource Domain Profile	The profile associated with the resource domain.	Format: Pulldown list Range: None, Alexa1, Alexa2 Range for PDRA: Policy Binding, Policy DRA, Policy Session
Server Groups	The server groups associated with the resource domain	Format: Checkbox Range: NO_MP, NO_SG, SO_MP, SO_SG Range for PDRA Policy Binding: NO Server Group, Site1BindingPsbrMpSg, Site1DsrMp1Sg, Site1DsrMp2Sg, Site1SessionPsbrMpSg, Site1SoServerGroup Range for Policy DRA: BindingPsbr1MpSg, IpfeServerGroup, LabCSOAMSG2, LABDDSRMSG, LabDSOAMSG, NOAMP_SG, PDRASG, SOAM_SG, SessionPsbr1MpSg Range for Policy Session: NO Server Group, Site1BindingPsbrMpSg, Site1DsrMp1Sg, Site1DsrMp2Sg, Site1SessionPsbrMpSg, Site1SoServerGroup

Inserting a Resource Domain

Use this procedure to insert a resource domain:

1. Select **Configuration > Resource Domains**.
2. Click **Insert** at the bottom of the table.

   The **Resource Domains Insert** page appears.

3. Enter a **Resource Domain Name**. This is a user-defined name for the domain. The domain name must be unique.
4. Select a **Resource Domain Profile**.
5. Select a **Server Group**.
6. Click **OK** to submit the information and return to the Resource Domains Configuration page, or click **Apply** to submit the information and continue entering additional data.

The resource domain is added to the network database.

Editing a Resource Domain

Use this procedure to edit resource domain information

1. Select **Configuration > Resource Domains**.
2. Select the resource domain from the listing.
3. Click **Edit** at the bottom of the table.

   The Edit Resource Domains page appears.

4. Modify one or more of the resource domain information fields.
5. Click **OK** to submit the information and return to the Resource Domains Configuration page, or click **Apply** to submit the information and continue editing additional data.

The resource domain information is updated in the network database and the changes take effect immediately.

Viewing Resource Domains

Use this procedure to view resource domains:

Select **Configuration > Resource Domains**.

The Resource Domains configuration page appears.

Deleting a Resource Domain

Use this procedure to delete a resource domain:

1. Select **Configuration > Resource Domains**.

   The **Resource Domains Configuration** page appears.

2. Click to select the resource domain you want to delete.

   Note: To prevent large service disruptions, you cannot delete a Resource Domain with a profile type or Policy Binding or Policy Session, unless the Policy DRA feature is deactivated. However, resource domains with a profile type of Policy DRA can be deleted without deactivation of the Policy DRA feature.

3. Click **Delete**.

   Click **Yes** to confirm.

The resource domain is deleted from the network database table.

Generating a Resource Domains Report

Use this procedure to generate a resource domains report:

1. Select **Configuration > Resource Domains**.
2. Click to select the resource domain for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.
   The resource domain group report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Places

The Places feature allows you to build associations for groups of servers at a single geographic location. These places can then be grouped into place associations, which create relationships between one or more place.

Places Insert elements

This table describes the elements of the Places Insert page.

Element	Description	Data Input Notes
Place Name	A unique name used to label the place.	Format: Alphanumeric characters and underscore "_" are allowed. A minimum of one alphabetic character is required. Range: Maximum length is 32 characters.
Parent	The parent place group that functions as the replication parent of the selected place	Format: Pulldown menu Any place that has no servers assigned is eligible to be a parent
Place Type	The place type.	Format: Pulldown menu Range: Site (default option) or defined by the application.
Servers	List of the available servers in the NO or SO	Format: Checkbox

Inserting a Place

Use this procedure to configure a place:

1. Select **Configuration > Places**.
2. Click **Insert**.

   The **Insert Places** page appears.

3. Enter the **Place Name.**

   For more information about **Place Name**, or any of the fields on this page, see Place Insert Elements.

4. Select a **Parent** from the pulldown menu.
5. Select a **Place Type** from the pulldown menu.
6. Select the available **Servers** from the checklist.
7. Click **OK** to submit the information and return to the Places page, or click **Apply** to submit the information and continue adding additional data.

Editing a Place

Use this procedure to edit place information

1. Select **Configuration > Places**.
2. Select the place from the listing.
3. Click **Edit** at the bottom of the table.

   The **Places Edit** page appears.

4. Modify one or more of the place information fields.
5. Click **OK** to submit the information and return to the Places page, or click **Apply** to submit the information and continue editing additional data.

The place information is updated in the network database and the changes take effect immediately.

Deleting a Place

Use this procedure to delete a place.

1. Select **Configuration > Places**.
2. Click to select the place you want to delete from the table.

   Note: A Place cannot be deleted if it includes servers or is a Parent Place. Before deleting, disassociate any servers or remove Parent status.

3. Click **Delete**.

   A delete confirmation message appears in a pop up window.

4. Click **OK** to delete the place.

   If you click **Cancel**, the place will not be deleted, and you will be returned to the **Places** page.

Generating a Places Report

Use this procedure to generate a places report:

1. Select **Configuration > Places**.
2. Click to select the place for which you want to create a report.

   Note: To select multiple servers, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.
   The place report appears.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Place Associations

The Place Association function allows you to create relationships between places. Places are groups of servers at a single geographic location.

Place Association Insert elements

This table describes the elements of the Place Association Insert page.

Element	Description	Data Input Notes
Place Association Name	A unique name used to label the place association.	Format: Alphanumeric characters and underscore "_" are allowed. A minimum of one alphabetic character is required. Range: Maximum length is 32 characters.
Place Association Type	The type of place association.	Format: Pulldown menu Range: defined by the application
Places	The places available to be grouped in this association	Format: Checkbox Range: list of places defined using Places function

Inserting a Place Association

Use this procedure to configure a place association:

1. Select **Configuration > Place Association**.
2. Click **Insert**.

The **Insert Place Associations** page appears.

3. Enter the **Place Association Name.**

   For more information about **Place Association Name**, or any of the fields on this page, see Place Association Elements.

4. Select a **Place Association Type** from the pulldown menu.
5. Click **OK** to submit the information and return to the Place Associations page, or click **Apply** to submit the information and continue adding additional data.

Editing a Place Associations

Use this procedure to edit place associations information

1. Select **Configuration > Place Associations**.
2. Select the place association from the listing.
3. Click **Edit** at the bottom of the table.

   The **Edit Place Associations** page appears.

4. Modify one or more of the place associations information fields.
5. Click **OK** to submit the information and return to the Place Associations Configuration page, or click **Apply** to submit the information and continue editing additional data.

The place association information is updated in the network database and the changes take effect immediately.

Deleting a Place Association

Use this procedure to delete a place association.

1. Select **Configuration > Place Associations**.
2. Click to select the place association you want to delete from the table.

   Note: You cannot delete a Place Association that includes grouped Places. Before deleting the Place Association, disassociate the Places from the Place Association

3. Click **Delete**.

   A delete confirmation message appears in a pop up window.

4. Click **OK** to delete the place association.

   If you click **Cancel**, the place association will not be deleted, and you will be returned to the Place Association page.

Generating a Place Associations Report

Use this procedure to generate a place associations report:

1. Select **Configuration > Place Associations**.
2. Click to select the place associations for which you want to create a report.
3. Click **Report**.

The place associations report appears.

4. Click **Print** to print the report, or click **Save** to save a text file of the report.

DSCP

The Differentiated Services Code Point (DSCP) pages allow the user to configure service point codes. Through the DSCP Configuration page, Interface and Port DSCP information can be inserted and saved to the configuration.

Interface DSCP

The Interface Differentiated Services Code Point (DSCP) pages allow the user to configure server interfaces for service point codes. Through the Interface DSCP Configuration page, DSCP information can be inserted and saved to the configuration.

Interface DSCP Insert elements

This table describes the elements of the Interface DSCP Insert page.

Table 60: Interface DSCP Insert Elements

Field	Description	Data Input Notes
Interface	The network interface name	Format: Drop down list Range: valid server interfaces
DSCP	DSCP value for the associated network interfaces	Format: Numeric Range: 0 to 63, inclusive
Protocol	TCP or SCTP protocol	Format: Drop down list

Inserting an Interface DSCP

Use the following procedure for inserting an interface DSCP.

1. Select **Configuration > DSCP > Interface DSCP**
   The Interface DSCP page appears.
2. Select the tab for Entire Network, NO_NE or SO_NE1.
3. Click the **Insert** button.
   The Insert Interface DSCP page appears.
4. Select the **Interface** from the drop down listing of available server interfaces.
5. Enter a valid **DSCP** value. A valid value is an integer between 0 and 63, inclusive.
6. Select **TCP or SCTP protocol** from the drop down list.

7. Click **OK** to submit the information and return to the DSCP page, or click **Apply** to submit the information and continue entering additional data.

The new DSCP is added.

Deleting an Interface DSCP

Use the following procedure for deleting an interface DSCP.

1. Select **Configuration > DSCP > Interface DSCP**
   The Interface DSCP page appears.
2. Select the DSCP configuration to be deleted.
3. Click **Delete**.
   A confirmation box appears.
4. Click **OK** to delete the DSCP
   The DSCP is deleted.

Generating an Interface DSCP Report

An interface DSCP report provides a summary of the configuration of one or more DSCPs. Reports can be printed or saved to a file.

1. Select **Configuration > DSCP > Interface DSCP**
   The Interface DSCP page appears.
2. Click **Report** to generate a report for all DSCPs.
   The DSCP Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Port DSCP

The Port Differentiated Services Code Point (DSCP) pages allow the user to configure server ports for service point codes. Through the Port DSCP Configuration page, DSCP information can be inserted and saved to the configuration.

Port DSCP Insert elements

This table describes the elements of the Port DSCP Insert page.

Table 61: Port DSCP Insert Elements

Field	Description	Data Input Notes
Port	A valid TCP or SCTP port	Format: Numeric Range: 1 to 65535, inclusive
DSCP	DSCP value for the associated port	Format: Numeric Range: 0 to 63, inclusive

Field	Description	Data Input Notes
Protocol	TCP or SCTP protocol	Format: Drop down list

Inserting a Port DSCP

Use the following procedure for inserting a Port DSCP.

1. Select **Configuration > DSCP > Port DSCP**
   The Port DSCP page appears.
2. Select the tab for Entire Network, NO_NE or SO_NE1.
3. Click the **Insert** button.
   The Insert Port DSCP page appears.
4. Enter a valid **Port** value. A valid value is an integer between 1 and 65535, inclusive.
5. Enter a valid **DSCP** value. A valid value is an integer between 0 and 63, inclusive.
6. Select **TCP or SCTP protocol** from the drop down list.
7. Click **OK** to submit the information and return to the DSCP page, or click **Apply** to submit the information and continue entering additional data.

The new DSCP is added.

Deleting a Port DSCP

Use the following procedure for deleting a Port DSCP.

1. Select **Configuration > DSCP > Port DSCP**
   The Port DSCP page appears.
2. Select the DSCP configuration to be deleted.
3. Click **Delete**.
   A confirmation box appears.
4. Click **OK** to delete the DSCP
   The DSCP is deleted.

Generating a Port DSCP Report

A Port DSCP report provides a summary of the configuration of one or more DSCPs. Reports can be printed or saved to a file.

1. Select **Configuration > DSCP > Port DSCP**
   The Port DSCP page appears.
2. Click **Report** to generate a report for all DSCPs.
   The DSCP Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Chapter 5

Alarms and Events

Topics:

This section provides an overview of alarms and events. Application alarms and events are unsolicited messages used in the system for trouble notification and to communicate the status of the system to Operations Services (OS). The application merges unsolicited alarm messages and unsolicited informational messages from all servers in a network and notifies you of their occurrence. Alarms enable a network manager to detect faults early and take corrective action to prevent a degradation in the quality of service.

Since alarms from each server are merged into one table of alarms at the SOAM and NOAMP servers, alarms should be viewed at the SOAM or NOAMP servers. When you log in to the GUI at the SOAM server, only alarms within that Network Element are visible. However, if you log in to the GUI at the NOAMP server, all alarms in the entire system are visible.

The **Alarms and Events** menu also features a page for viewing and generating reports of SNMP traps.

Alarms and events defined

Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. An alarm might represent a change in an external condition, for example, a communications link has changed from connected to a disconnected state. Alarms can have these severities:

- Critical
- Major
- Minor
- Cleared - An alarm is considered inactive once it has been cleared, and cleared alarms are logged on the **Alarms & Events > View History** page.

Events note the occurrence of an expected condition, such as an unsuccessful login attempt by a user. Events have a severity of Info and are logged on the **View History** page.

The following figure shows how alarms and events are organized in the application.

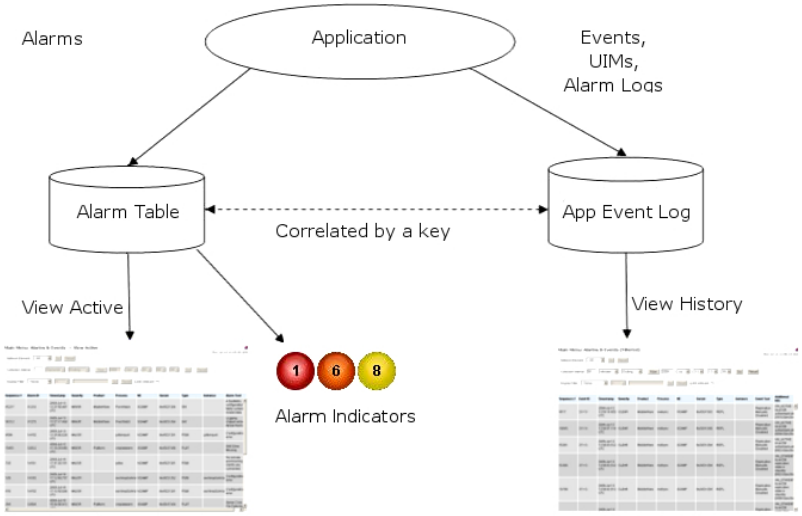


Figure 15: Flow of Alarms

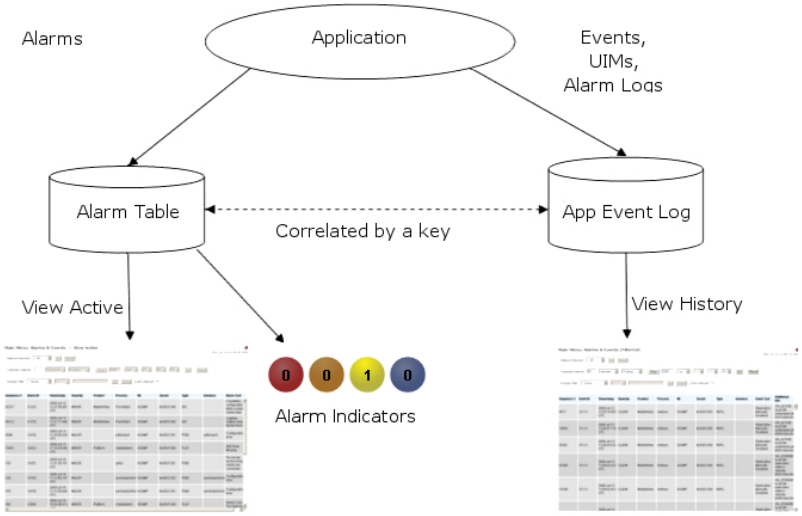


Figure 16: Flow of Alarms

Alarms and events are recorded in a database log table. Application event logging provides an efficient way to record event instance information in a manageable form, and is used to:

- Record events that represent alarmed conditions
- Record events for later browsing
- Implement an event interface for generating SNMP traps

Alarm indicators, located in the User Interface banner, indicate all critical, major, and minor active alarms. A number and an alarm indicator combined represent the number of active alarms at a specific level of severity. For example, if you see the number six in the orange-colored alarm indicator, that means there are six major active alarms.

●	Active Critical Alarm (bright red)
●	Active Major Alarm (bright orange)
●	Active Minor Alarm (bright yellow)
●	No active Critical Alarm (pale red)
●	No active Major Alarm (pale orange)
●	No active Minor Alarm (pale yellow)
○	Not Connected (white)

Figure 17: Alarm Indicators Legend

●	Trap count > 0 (bright blue)
●	Trap count = 0 (pale blue)

Figure 18: Trap Count Indicator Legend

Alarm and event ID ranges

The **AlarmID** listed for each alarm falls into one of the following process classifications:

Table 62: Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5099
OAM	10000-10999
IDIH	11500-11549
SBR	12000-12999
ComAgent	19800-19909
DSR Diagnostics	19910-19999
Diameter	22000-22350, 22900-22999
RBAR	22400-22424
Generic Application	22500-22599
FABR	22600-22640
PDRA	22700-22799
CPA	22800-22849
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
DM-IWF	33000-33024
Load Generator	33025-33049
MD-IWF	33050-33099
GLA	33100-33149

Alarm and event types

This table describes the possible alarm/event types that can be displayed.

Note: Not all applications use all of the alarm types listed.

Table 63: Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
CPA	Charging Proxy Application
DAS	Diameter Application Server (Message Copy)
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability
HSS	Home Subscriber Server
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NP	Number Portability
OAM	Operations, Administration & Maintenance
PDRA	Policy DRA
pSBR	Policy SBR

Type Name	Type
PLAT	Platform
PROC	Process
PROV	Provisioning
NAT	Network Address Translation
RBAR	Range-Based Address Resolution
REPL	Replication
SBRA	Session Binding Repository Application
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

Active alarms elements

This table describes the elements on the **View Active** alarms page.

Table 64: Active Alarms Elements

Active Alarms Element	Description
Sequence #	A system-wide unique number assigned to each alarm
Alarm ID	A unique number assigned to each alarm in the system. See *Alarm and event ID ranges* for more information.
Alarm Text	Description of the alarm. The description is truncated to 140 characters. **Note:** The **Alarm Text** field is not truncated in exports or reports.

Active Alarms Element	Description
Timestamp	Date and time the alarm occurred (fractional seconds resolution)
Severity	Alarm severity - Critical, Major, Minor
Product	Name of the product or application that generated the alarm
Process	Name of the process that generated the alarm
NE	Name of the Network Element where the alarm occurred
Server	Name of the server where the alarm occurred
Type	Alarm or Event Type, e.g. Process, Disk, Platform. See *Alarm and event types* for more information.
Instance	Instance of the alarm, e.g. Link01 or Disk02. The Instance provides additional information to help differentiate two or more alarms with the same number. This field may be blank if differentiation is not necessary

Viewing active alarms

Active alarms are displayed in a scrollable, optionally filterable table. By default, the active alarms are sorted by time stamp with the most recent alarm at the top.

Use this procedure to view active alarms.

Note: The alarms and events that appear in **View Active** vary depending on whether you are logged in to an NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

1. Select **Alarms & Events > View Active**.
   The **View Active** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.

   The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.

3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

   If a new alarm is generated while automatic updates are suspended, a new message appears: `(Alarm updates are suspended. Available updates pending.)`

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Active alarms data export elements

This table describes the elements on the **View Active Export** alarms page.

Table 65: Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting active alarms

You can schedule periodic exports of alarm data from the **Alarms and Events View Active** page. Active alarm data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View Active** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Alarm details can be exported to a file by clicking the **Export** button on the **View Active** page. The system automatically creates and writes the exported active alarm details to a CSV file in the file management area.

If filtering has been applied in the **View Active** page, only filtered, active alarms are exported.

Use this procedure to export active alarms to a file.Use this procedure to schedule a data export task.

1. Select **Alarms & Events > View Active**.
   The **View Active** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Active Alarm Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Active alarms data export elements* .
5. Select the **Export Frequency**.
6. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

7. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

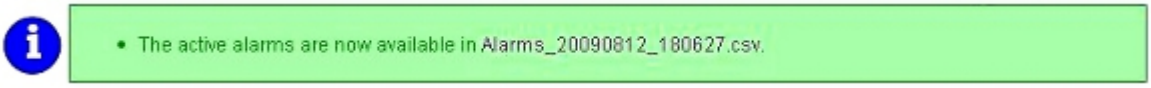
8. Click **OK** or **Apply** to initiate the active alarms export task.

   From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*
   - *Deleting a scheduled task*
   - *Generating a scheduled task report*

9. Click **Export**.
   The file is exported.
10. Click the link in the green message box to go directly to the **Status & Manage > Files** page.



From the **Status & Manage > Files** page, you can view a list of files available for download, including the active alarms file you exported during this procedure.

Generating a report of active alarms

Use this procedure to generate a report.

1. Select **Alarms & Events > View Active**.

   The **View Active** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The active alarms are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.
3. Click **Report**.
   The View Active Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Historical alarms and events elements

This table describes the elements on the **View History** alarms and events page.

Table 66: Historical Alarms Elements

Historical Alarms Element	Description
Sequence #	A system-wide unique number assigned to each alarm/event.
Event ID	A unique number assigned to each alarm/event in the system.
Event Text	Description of the alarm/event. The description is truncated to 140 characters. If the description is truncated, a link to the alarm report will be appended.
Timestamp	Date and time the alarm/event occurred (fractional seconds resolution).
Severity	Alarm/event severity - Critical, Major, Minor and Info.

Historical Alarms Element	Description
Additional Info	Any additional information about the alarm/event that might help fix the root cause of the alarm/event. **Additional Information** is truncated to 140 characters. **Note: Additional Info** field is not truncated in exports or reports.
Product	Name of the product or application that generated the alarm/event.
Process	Name of the process that generated the alarm/event.
NE	Name of the Network Element where the alarm/event occurred.
Server	Name of the server where the alarm/event occurred.
Type	Alarm or Event Type, e.g. Process, Disk, Platform. See *Alarm and event types* for more information.
Instance	Instance of the alarm/event, e.g. Link01 or Disk02. The Instance provides additional information to help differentiate two or more alarms/events with the same number. This field may be blank if differentiation is not necessary.

Viewing alarm and event history

All historical alarms and events are displayed in a scrollable, optionally filterable table. The historical alarms and events are sorted, by default, by time stamp with the most recent one at the top. Use this procedure to view alarm and event history.

Note: The alarms and events that appear in **View History** vary depending on whether you are logged in to an NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

1. Select **Alarms & Events > View History** .
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.

   Note: Some fields, such as **Additional Info**, truncate data to a limited number of characters. When this happens, a **More** link appears. Click **More** to view a report that displays all relevant data.

   Historical alarms and events are displayed according to the specified criteria.

   The historical alarms table updates automatically. When new historial data is available, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.

The following message appears: `(Alarm updates are suspended.)`

If a new alarm is generated while automatic updates are suspended, a new message appears: `(Alarm updates are suspended. Available updates pending.)`

To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Historical events data export elements

This table describes the elements on the **View History Export** page.

Table 67: Schedule Event Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button

Element	Description	Data Input Notes
		Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting alarm and event history

You can schedule periodic exports of historical data from the **Alarms and Events View History** page. Historical data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View History** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

The details of historical alarms and events can be exported to a file by clicking the **Export** button on the **View History** page. The system automatically creates and writes the exported historical alarm details to a CSV file in the file management area.

If filtering has been applied in the **View History** page, only filtered historical alarms and events are exported. Use this procedure to export alarm and event history to a file. Use this procedure to schedule a data export task.

1. Select **Alarms & Events > View History**.
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Event Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Historical events data export elements* .
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

8. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

9. Click **OK** or **Apply** to initiate the data export task.

   The data export task is scheduled. From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see *Displaying the file list*.

Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

- *Viewing scheduled tasks*
- *Editing a scheduled task*
- *Deleting a scheduled task*
- *Generating a scheduled task report*

10. Click **Export**.
    The file is exported.
11. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see .

Generating a report of historical alarms and events

Use this procedure to generate a report.

1. Select **Alarms & Events > View History**.

   The **View History** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Report**.
   The View History Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

View Trap Log

The **View Trap Log** page allows you to monitor traps from external application equipment, such as switches and enclosures. The purpose of monitoring traps is to gain early warning of possible service impacting conditions. **View Trap Log** provides a visual indicator of active, existing conditions. It also provides a detailed log recording the historical conditions present in the external monitored hardware and important background information for investigating the root cause of the condition.

View Trap Log elements

This table describes the elements on the **View Trap Log** page.

Table 68: View Trap Log Elements

Element	Description
Timestamp	The timestamp (in UTC) when the trap record was collected on the current system.
OID	The Object Identifier (OID) for the trap.
upTime	The uptime as reported by the monitored external equipment.
Trap Collector	The name of the server that first logged the trap.
Trap Source	The external hostname (or IP, if name cannot be resolved) for the trap source.
VarBinds	The OID/value pairs found in the varbind list. **Note:** Only the first few OID/value pairs will be displayed. A link to the report for the record will be added if the varbind list is truncated.
Acknowledge All **Acknowledge**	When the **Acknowledge All** button is clicked, up to 2000 traps selected by the filter are cleared. Acknowledged traps are removed from both the trap count indicator and the **View Trap Log** page. **Note: Acknowledge All** is the default setting for this button. When one or more traps are selected, the button toggles to **Acknowledge**, and only the selected traps are affected.
Unacknowledge All **Unacknowledge**	When the **Unacknowledge All** button is clicked, all previously acknowledged traps selected by the filter reappear on the page. Unacknowledged traps are added to the trap count indicator. **Note: Unacknowledge All** is the default setting for this button. When one or more traps are selected, the button toggles to **Unacknowledge**, and only the selected traps are affected.
Report All **Report**	When the **Report All** button is clicked, a report is generated that contains information about the first 25 traps selected by the filter. **Note: Report All** is the default setting for this button. When one or more traps are selected, the button toggles to **Report**, and only the selected traps are included in the report.

Element	Description
Show: Ack'ed	Selection of this checkbox shows (if checked) or hides (if unchecked) the acknowledged trap records. **Note:** This checkbox is a filter option that is only available on the **View Trap Log** page.

Viewing trap logs

Trap logs are displayed in a scrollable, optionally filterable table.

1. Select **Alarms & Events > View Trap Log**.
   The **View Trap Log** page appears.
2. If necessary, specify filter criteria and click **Go**.
3. If necessary, click to select any traps you want to acknowledge.

   Note: Acknowledging a trap will cause the trap to be removed from the table and from the trap count indicator. For more information, see *View Trap Log elements* .

   Alternately, click **Acknowledge All** to acknowledge all traps, or click **Unacknowledge All** to show all traps in the table once again.

   The trap log table updates automatically. When new traps are available, the table is automatically updated, and the view returns to the top row of the table.

4. To suspend automatic updates, click any row in the table.
   The following message appears: `(SNMP Trap updates are suspended.)`

   If a new trap is generated while automatic updates are suspended, a new message appears: `(SNMP Trap updates are suspended. Available updates pending.)`

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

View Trap Log Report elements

This table describes the elements on the **View Trap Log Report** page.

Table 69: View Trap Log Report Elements

Element	Description
acked	Indicates whether the trap has been acknowledged. Value = True or False

Element	Description
duplicate	Indicates whether the trap has been marked as a duplicate. Value = True or False
trapId	The trap ID is an internal sequence number to identify specific traps from the same source.
OID	The Object Identifier (OID) for the trap.
upTime	The upTime as reported by the monitored external equipment.
srcNode	The name of the server that first logged the trap.
networkElement	The Network Element of the server that first logged the trap.
timeStamp	The timestamp (in UTC) when the trap record was collected on the current system. **Note:** This is the timestamp used when specifying the collection interval.
srcTimeStamp	The time (in UTC) when the specific trap record was received at the system that first logged the trap.
Trap Source	The external hostname (or IP, if name cannot be resolved) for the trap source.
trapSourceIP	The IP address of the external hardware being monitored.
varbind	The specific OID/value pairs found in the varbind list. There will be a varbind entry for each varbind in the logged trap record.

Generating a trap log report

Use this procedure to generate a report..

1. Select **Alarms & Events > View Trap Log**.
   The **View Trap Log** page appears.
2. Click to select the trap log for which you want to create a report.

   Note: If no trap is selected, the report will contain data about the first 25 traps selected by the filter. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.

   Note: When no trap is selected, the button toggles to **Report All**.

The **View Trap Log Report** page appears.

4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Chapter 6

Security Log

Topics:

This section provides an overview of security log options. The **Security Log** page allows you to view the historical security logs from all configured servers. Security logs are displayed in a scrollable, optionally filterable table. Security log data can be exported and then retrieved from the **Status & Manage > Files** page.

The **Export** function allows you to export security log files from one or more servers to the file management storage area of the server to which your GUI session is connected. Files in the file management storage area can be viewed from the **Status & Manage > Files** page. The logging feature is an OAM function, so you can be connected to either a NOAMP server or an SOAM server (but not an MP server).

The system automatically creates and writes the exported security log details to a CSV file in the file management area, as the following figure shows. If filtering has been applied in the **View Active** page, only filtered active alarms are exported.

CSV files can be downloaded from the file management storage area to your computer, such as your client PC, using the **Status & Manage > Files** page. See *Files* for steps on how to download files to your computer.

Security Log View History elements

This table describes the elements of the **Security Log > View History** page.

Table 70: Security Log View History Elements

Security Log History Element	Element Description
Timestamp	The date and time the security record was generated (fractional seconds resolution).
User	The user initiating the action.
Sess ID	The session identifier.
Remote IP	The remote IP address for the user.
Message	Summary details about the action which generated the security record.
Status	The status of the action, either SUCCESS or ERROR.
Screen	The page on which the action occurred, the Login page, for example.
Action	The user action, login, for example.
Details	Additional details about the action which generated the security record.
Server	The server which processed the action.

Viewing security log files

Use this procedure to view security log files.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. Specify the **Collection Interval**.
3. If necessary, specify filter criteria and click **Go**.

   Note: Some fields, such as **Details**, truncate data to a limited number of characters. When this happens, a **More** link appears. Click **More** to view a report that displays all relevant data.

The security log history displays sorted by collection time stamp.

Note: There are two relevant time stamps for the security log: the time stamp of the event and the time stamp for when the record was merged. The time stamps display initially using the source time, which makes the report appear unordered. However, the report is indeed sorted by collection time.

Security log data export elements

This table describes the elements on the **View History Export Security Log** page.

Table 71: Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Once, Hourly, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Export Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Textbox or Scrolling List Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Scrolling List Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting security log files

You can schedule periodic exports of security log data from the **Security Log View History** page. Security log data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View History** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to export security log files.Use this procedure to schedule a data export task.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The security log files are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Security Log Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Security log data export elements* .
5. Enter a **Description** for the export task.
6. Select the **Export Frequency**.
7. If you selected Hourly as the export frequency, select the **Minute** of each hour for the data export.
8. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

9. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

10. Click **OK** or **Apply** to initiate the security log export task.

    From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

    Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

    - *Viewing scheduled tasks*
    - *Editing a scheduled task*
    - *Deleting a scheduled task*
    - *Generating a scheduled task report*

11. Click **Export**.
    The file is exported.
12. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the security log history you exported during this procedure.

If an export fails for any reason, an error message appears indicating this failure.

Generating a Security Log report

Use this procedure to generate a report.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. Specify the **Collection Interval**.
3. Specify the filter criteria, if necessary, and click **Go**.
   The security log files are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.
4. Click **Report**.
   The Security Log Report is generated. This report can be printed or saved to a file.
5. Click **Print** to print the report.
6. Click **Save** to save the report to a file.

Chapter 7

Status and Manage

Topics:

This section describes how to view and manage the various types of data generated by the system.

Network Elements

The Network Elements page provides the status of network elements as well as a location in which you can manage Customer Router Monitoring. Customer Router Monitoring, if enabled, monitors connectivity from the system to customer network gateways.

Network elements status elements

This table describes the elements of the **Status & Manage > Network Elements** page.

Table 72: Network Elements Status Elements

Network Elements Status Element	Description
Network Element Name	The network element name associated with each server hostname. Each configured network element in the system is listed here.
Customer Router Monitoring	Indicates whether router monitoring is enabled or disabled.
Enable Ping	A button that enables Customer Router Monitoring for the selected network element.
Disable Ping	A button that disables Customer Router Monitoring for the selected network element.

Enabling and disabling ping on Network Elements

This procedure describes how to enable or disable Customer Router Monitoring on selected Network Elements.

1. Select **Status & Manage > Network Elements**.
   The **Network Elements Status & Manage** page appears.
2. Click to select a Network Element.
3. Click **Enable Ping** to enable Customer Router Monitoring, or click **Disable Ping** to disable Customer Router Monitoring.

   A confirmation window appears.
4. Click **OK** to continue.

   A progress bar that displays the message "Please wait..." appears.

A message appears in the **Information** area of the screen to confirm the success of the procedure. The Customer Router Monitoring status has been changed.

If the procedure fails, an error message appears. Repeat steps *Step 2* through *Step 4*. If the problem persists, contact My Oracle Support.

Server

The **Server** page provides a single point for monitoring collected data, isolating problems, and performing actions required for server maintenance. This page provides roll-up status for six subsystems on each server defined in the network. You can navigate to individual subsystem status pages for more detailed information with a single click on the **Server** page.

Server status elements

This table describes the elements on the **Status & Manage > Server** page.

Table 73: Server Status Elements

Server Status Element	Description
Network Element	The network element name associated with each Server Hostname.
Server Hostname	The server hostname. All servers in the system are listed here.
Appl State	An administrative state that reflects the state of the application running on each server. Possible states are Enabled, Disabled, and Unk (Unknown indicates the application state cannot be determined due to an error).
Alm	Aggregated alarm status for each server. Possible values are Norm, Err, Warn, and Unk.
DB	Aggregated database status for each server. Possible values are Norm, Err, Warn, Unk, and Man.
Reporting Status	Reporting status for each server. Possible values are Norm, Err, Warn, Unk, and Man.
Proc	Aggregated process status for each server. Possible values are Norm, Err, Unk, and Man.

Server Status

Each server collects performance data and status information for several subsystems. Since the system may consist of hundreds of geographically diverse servers, you need the ability to monitor this data and quickly isolate problems.

There are several aspects to monitoring server status. You can monitor the administrative state of each server in the system, as well as the status of the alarms, replication, collection, high availability, database, and process systems on each server.

The **Application State** field for each server displays the current administrative state of the application running on that server. Stopping application software places it in the Disabled **Application State**. Restarting application software places it in the Enabled **Application State**. Servers that are restarted by clicking **Restart** will restart all application processes, regardless of their current state.

Note: Enabled and Disabled are administrative states. They do not reflect the current status or running state of the application software.

The Collection subsystem gathers status and alarm information from all other subsystems. Each of these subsystems reports varying degrees and severities of status. The status reported is not the same between subsystems. For this reason, the **Server Status** page provides a common status reporting framework to help identify problems at a server level.

Reporting status framework

This table describes the reporting framework:

Table 74: Reporting Status Framework

Reporting Status	Description
Norm (Normal)	The subsystem is operating as expected.
Warn (Warning)	The subsystem is experiencing one or more minor problems.
Err (Error)	The subsystem is experiencing one or more Major or Critical problems.
Man (Manual Maintenance)	The subsystem has been placed in a manually assigned state.
Unk (Unknown)	No information is available for the subsystem. When there is a problem gathering data in the Alarm, HA, or Database subsystems, the Collection subsystem sends a status of *unknown*.

Not all of the subsystems report status per server. The HA Status subsystem shares some status information between two servers. The **Server** page combines status information into a single status per subsystem per server.

How status is reported for each subsystem is explained in more detail in these sections:

- *Alarm status elements*
- *HA status elements*
- *Database status elements*
- *Process status elements*

Alarm status elements

Alarm status is derived from all of the alarms present on a server. For information on the alarms subsystem, see *Alarms and events defined* . This table describes the possible alarm severities and their equivalent reporting statuses on the **Server** page.

Table 75: Alarm Status vs Reporting Status

Alarm Status	Reporting Status Equivalent	Priority	Color
Unknown	Unk	1 (highest)	Red
Critical	Err	2	Red
Major	Err	3	Orange
Minor	Warn	4	Yellow
None	Norm	5 (lowest)	-

Database status elements

The **Server** page combines the individual status, maintenance, and the collection delivery mechanism into a single database status. The highest priority status is the one reported to the **Server** page.

Note: *Unknown* is the status reported when a failure prevents the reporting or the collection of database status.

Table 76: Database Status vs Reporting Status

Database Status	Reporting Status Equivalent		Priority	Color
	Maintenance in Progress	Maintenance NOT in Progress		
Unknown	Unk	Unk	1 (highest)	Red
Critical	Man	Err	2	Red
Major	Man	Err	3	Red
Minor	Man	Warn	4	Yellow
Normal	Man	Norm	5 (lowest)	-

HA status elements

HA Status is derived from the **HA Status** and **HA Availability** fields on the **HA Status** page. The collection mechanism is combined with status and availability but not with the forced standby state.

The **Server** page reports High Availability manual maintenance status (forced standby) differently from other status subsystems. Most manual maintenance statuses are stored on the affected server, collected to the reporting server, and displayed. The forced standby state is replicated rather than collected, and is therefore available directly on the reporting server.

Note: *Unknown* is the status reported when a failure prevents the reporting or the collection of HA availability.

Table 77: HA Status vs Reporting Status

HA Status	Reporting Status Equivalent		Priority	Color
	Forced Standby	NOT Forced Standby		
Unknown	Man	Unk	1 (highest)	Red
Offline	Man	Err	2	Red
Failed	Man	Err	3	Red
Degraded	Man	Warn	4	Yellow
Normal	Man	Norm	5 (lowest)	-

Process status elements

The **Server** page combines the individual process status and the collection delivery mechanism into a single process status. The highest priority status is the one reported to the **Status** page. Processes which are intentionally not running on the server do not show up in process status.

Note: *Unknown* is the status reported when a failure prevents the reporting or the collection of process status.

Table 78: Process Status vs Reporting Status

Process Status	Reporting Status Equivalent		Priority	Color
	Application Disabled	Application Enabled		
Unknown	Man	Unk	1 (highest)	Red
Pend	Man	Err	2	Red
Kill	Man	Norm	3	-
Up	Man	Norm	4 (lowest)	-

Server errors

There are three ways to view servers with alarm status other than Normal:

- **Viewing the Server Status page**: All servers appear on this page along with the highest alarm for each subsystem.
- **Mousing over an aggregated server status**: The underlying status reported by the subsystem appears when the cursor moves over that status.
- **Viewing the aggregated server status**: The aggregated status for each subsystem is a link to the selected subsystem's page. The page provides details for the selected server only. Click on the link to view the status for the selected server.

Aggregated server status elements

Clicking a status link opens the status page that corresponds to the selected column and filters that page by the server corresponding to the selected row.

Table 79: Click-Through Status Screen

Server Status Column	Corresponding Status Page
Alm	**Alarm History** Page - see *Viewing alarm and event history*
DB	**Database Status** Page - see *Database*
HA	**High Availability Status** Page - see *HA (High Availability)*
Proc	**Processes Page** - see *Processes*

Displaying aggregated server status

Use this procedure to display a corresponding status page:

1. Select **Status & Manage > Server**.

   The **Server Status** page appears.

2. Click the status field for which you want to view more details.

The related status page appears with only the selected server in the status table.

Stopping the application

Use this procedure when the application on a server needs to be stopped. Stopping the application software places it in the Disabled Application state. Examples of when to stop the application include times when you need to delete a server, change a server role, or perform a system restore.

GUI sessions are not affected by the stop and restart application software actions. You may continue to use the GUI as these actions progress. You may use GUI sessions connected to servers with stopped application software. GUI provisioning may be affected if the server is the active NOAMP server. Stopping and starting application software may cause a switchover as well; you can observe changes in the status of those servers from the **Server Status** page.

WARNING

Warning: Do not click **Stop** for an application until you have assessed the impact on the system. Stopping the application on a server can adversely affect processes on this server and/or other servers in the network element.

1. Select **Status & Manage > Server**.

   The **Server Status** page appears.

2. Click to select the server you want to stop.

Alternately, you can select multiple servers to stop. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click **Stop**.

   A warning message appears:

   Are you sure you wish to stop application software on the following server(s)? <server name>

4. Click **OK** to continue.

Application processes are disabled on this server. Stopping the application or restarting running software influences the High Availability subsystem by raising an alarm. Stopping application software affects server processing in the following ways:

- Servers continue to emit alarms and collect measurements.
- NOAMP and SOAM servers continue to publish replicated data and accept GUI connections.
- SOAM and Message processing servers continue to subscribe to replicated data.
- NOAMP servers do not accept provisioning/configuration changes.
- MP servers do not maintain signaling connections nor process messages.

Restarting the application

If the **Application State** displays Disabled, **Restart** starts the software. If the **Application State** displays Enabled, **Restart** stops and then starts the software. Restarting the software places it in the enabled state.

A Restart can be used:

- To restart a newly created server, which has software in the disabled state.
- When a server is removed and re-added to topology and has software in the disabled state.

GUI sessions are not affected by the restart application software action. You may continue to use the GUI as these actions progress. You may use GUI sessions connected to servers with application software being restarted. GUI provisioning may be affected if the server is the active NOAMP server. Stopping and starting application software may cause a switchover as well; you can observe changes in the status of these servers from the **Server Status** page.

WARNING

Warning: Do not click **Restart** for an application until you have assessed the impact on the system. Restarting the application on a server can adversely affect processes on this server and/or other servers in the network element.

Use this procedure to restart the application on a server:

1. Select **Status & Manage > Server**.

   The Server Status page appears.

2. Click to select the server you want to restart.

   Alternately, you can select multiple servers to restart. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click **Restart**

   A warning message appears:

   Are you sure you wish to restart application software on the following server(s)? <server name>

4. Click **OK** to continue.

Application processes are restarted on this server. Restarting running software influences the High Availability subsystem by raising an alarm. If the software is running when the Restart is selected, the stopping of the software affects server processing in the following ways:

- Servers continue to emit alarms and collect measurements.
- NOAMP and SOAM servers continue to publish replicated data and accept GUI connections.
- SOAM and Message processing servers continue to subscribe to replicated data.
- NOAMP servers do not accept provisioning/configuration changes.
- Message Processing servers do not maintain signaling connections nor process messages.

Rebooting a server

A server should not be rebooted until you have assessed the full impact on the system. This list describes what happens when servers of different roles are rebooted:

- **OAM Server controlling GUI session:** Reboot of OAM Servers ends all GUI sessions controlled by that server. Note that the reboot may reboot the server controlling your GUI session. After the reboot sequence completes, you can re-establish a GUI session with the rebooted server. You are presented with a login screen and will need to re-authenticate to create a new session.
- **Active OAM Server:** Stopping and starting application software may cause a switchover. You have different capabilities on Active vs. Standby OAM servers, depending on the feature. For example, provisioning is only allowed from the Active NOAMP server.
- **Other Servers:** Rebooting Message Processing servers and Standby OAM servers without GUI sessions has no direct GUI impact. You can observe changes in the status of these servers. A BR tag was used here in the original source.

WARNING

Warning: Do not click **Reboot** for a server until you have assessed the impact on the system. **Reboot** temporarily halts all services on the designated server; do not perform a Reboot unless other servers within the network element can take over the traffic load.

Use this procedure to reboot a server:

1. Select **Status & Manage > Server**.

   The **Server Status** page appears.

2. Click to select the server you want to reboot.

   Alternately, you can select multiple servers to reboot. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click **Reboot**.

   A warning message appears:

   Are you sure you wish to reboot the following server(s)? <server name>

4. Click **OK** to continue.

The specified server is rebooted. Rebooting the server influences the High Availability subsystem. The rebooted server's mate no longer detects HA heartbeats and raises an alarm.

HA (High Availability)

HA Status provides the status of the HA relationships for OAM and MP servers, which are configured to run as either active-standby server pairs or individual servers. The internal status fields are used to map to a Derived HA Status. The Derived HA Status is displayed as the HA Status.

The Availability state of a server is used by HA to determine when a switchover is necessary. Availability is ranked with a score. A lower score is better and means the server is in better health. The decision to switchover is based on this score. The switchover will only occur if a Standby server is deemed to be in better health (has a lower score) than an Active server. If the Standby's score is equal to or higher than the Active's score, then a switchover does not occur. In the HA Status screen, the server taking over shows its HA Status going to Active and HA Role going to Providing Service. The mate will show its unhealthier status.

Availability states are driven from conditions or events which have occurred on a server. As events and conditions change on a server, its Availability status can change. Depending on the set of conditions on an Active-Standby server pair, a switchover may occur.

HA status elements

The **HA** page displays detailed status of how HA is working in the entire network in tabular form. This table describes the details displayed for all servers:

Table 80: HA Status Elements

HA Status Element	Description
Hostname	The server's hostname.
OAM Max HA Role	The observed maximum high availability role among all resources in policy 0 on the server: • Active: Server is running as the Active server. It is providing service and owns the VIP. • Standby: Server is running as the Standby server. It is ready to provide service in the event of a switch over. • Spare: Server is running as the Spare server. • Observer: Server is running as the Observer server. • OOS: Server is out of service.
Application Max HA Role	The observed maximum HA role among all resources in all other policies on the server: • Active: Server is running as the Active server. It is providing service and owns the VIP. • Standby: Server is running as the Standby server. It is ready to provide service in the event of a switch over.

HA Status Element	Description
	• Spare: Server is running as the Spare server. • Observer: Server is running as the Observer server. • OOS: Server is out of service.
Max Allowed HA Role	The maximum allowed HA role that the server is expected to achieve across all policies: Defaults are: • NOAMP: Active • SOAM: Active • MP: Active • Query Server: Observer
Mate Hostname List	List of possible hostnames that can act as the server's mate.
Network Element	The network element that the server belongs to.
Server Role	The server's role (, Query Server, or MP for Message Processor).
Active VIPs	An indication of all VIPs that are active on the server

Viewing HA status data

Use this procedure to view HA status data:

Select **Status & Manage > HA**.

The **HA Status** page appears.

Modifying the HA Status

Use this procedure to modify the HA status:

1. Select **Status & Manage > HA**.

   The HA Status and Manage page appears.

2. Click **Edit**.
3. Change the **Max Allowed HA Role** for any hostname on the list.

   Note: At least one NOAMP must remain active on the network.

4. Click **Ok** to save the changes.

The modifications are written to the database. The change takes effect immediately.

Sorting HA status data

HA status data is not displayed in a particular default order. To sort the HA status data, click on any of the column headers in the HA status table to sort the table by that column. Clicking again on the same column header reverses the direction of the sort (ascending or descending). To return to the table's original ordering, click **Status & Manage > HA**.

Database

The **Database** page provides:

- The ability to disable and enable provisioning system-wide on active NOAMPs and site-wide on the active SOAM.
- Database status information for each server in the network. The system tracks alarms associated with a database and displays this information on the **Database** page.
- Access to several database functions. These functions include: inhibiting and restoring provisioning and configuration updates to the system; backing up and restoring a database (and the status of these functions); displaying a database status report; inhibiting/allowing replication; and comparing a backed up and archived database to an existing database. With the exceptions of restore and replication, these functions affect a single OAM server only.
- The status of database backups.
- The durability status.

Database status elements

The **Database** page displays status information and functions on a per server basis. This table describes the elements on the **Status & Manage Database** page.

Note: At the top of the Database Status and Manage screen is an **Info** display. Database maintenance operations, for example, automatic and manual backups, or restore messages, are listed in this information display. While not technically a status table element, this display provides important information and should be viewed periodically.

Table 81: Database Status Elements

Element	Description
Network Element	The name of the Network Element to which the server belongs.
Server	Name of the Server.
Role	The role the server plays in the system.
OAM Max HA Role	The observed maximum high availability role among all resources in policy 0 on the server: • Active: Server is running as the Active server.

Element	Description
	• Standby: Server is running as the Standby server. It is ready to provide service in the event of a switch over. • Spare: Server is running as the Spare server. • Observer: Server is running as the Observer server. • OOS: Server is out of service.
Application Max HA Role	The observed maximum HA role among all resources in all other policies on the server: • Active: Server is running as the Active server for application policies. • Standby: Server is running as the Standby server. It is ready to provide service in the event of a switch over. • Spare: Server is running as the Spare server. • Observer: Server is running as the Observer server. • OOS: Server is out of service.
Status	Alarm status for a server; status is reported for a server as the highest severity of all database alarms associated with that server. The status of the server affects the color of that server row: • Normal - No alarms related to DB status (no change in background color). • Minor - The server has raised a minor alarm that relates to DB status (yellow background). • Major - The server has raised a major alarm that relates to DB status (orange background). • Critical - The server has raised a critical alarm that relates to DB status (red background). • Unknown - Alarm collection is not possible or reports an error (red background).
DB Level	The database update level on a server. This value is incremented by certain types of database updates and allows the user to compare DB levels across different servers.
OAM Repl Status	OAM Replication status for a server as reported by COMCOL: • Unknown - no current status information. • Normal - all links are normal. • Degraded - some replication links are up, some are down.

Element	Description
	• Failed - all replication links to this server are down or failed. • Not Applicable - replication does not apply. • Not Configured - replication is not configured. • Auditing - all links are auditing or normal, zero links are down.
SIG Repl Status	Signaling Replication status for a server as reported by COMCOL: • Unknown - no current status information. • Normal - all links are normal. • Degraded - some replication links are up, some are down. • Failed - all replication links to this server are down or failed. • Not Applicable - replication does not apply. • Not Configured - replication is not configured. • Auditing - all links are auditing or normal, zero links are down.
Repl Status	Displays whether replication is inhibited for the server. The inhibiting of replication on servers occurs automatically during the Restore procedure.
Repl Audit Status	Displays whether replication auditing is in progress for the server.

Viewing database status

The **Database Status** page displays a table of all servers and their associated database status. In order to identify servers that require attention, information for each database is condensed into a single status, which is shown in the **Status** column. The database alarm status indicates the severity of the most severe database-related alarm on each server. This status affects the color of the background for the server status cell. For more details on the **Status** element and a description of the background colors, see the **Status** description in the table in the previous section, *Database status elements* .

Use the following procedure to view the database status for servers:

Select **Status & Manage > Database**.

Sorting database data

Database data is not displayed in a particular default order. To sort the database data, click on any of the column headers in the Database status table to sort the table by that column. Clicking again on the same column header reverses the direction of the sort (ascending or descending).

Generating the server database report

The Server Database Report provides detailed information about a selected server, such as:

- Name of the server on which the report is generated
- Any associated database alarms
- Any associated database maintenance in progress
- Current database disk and memory utilization
- Other service information of use to My Oracle Support personnel when diagnosing a problem

Use this procedure to generate a server database report:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click to select the server for which you want to generate a report.
3. Click **Report**.

   The Database Report for the selected server appears on a new page.

4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Inhibiting/Allowing replication of data

The **Database Status** page provides manual control for inhibiting and re-allowing database replication on servers.

Note: The inhibiting of replication on servers occurs automatically during the Restore procedure. For information on this process, see *Restoring data to the active NOAMP server*.

Use this procedure to inhibit replication on a server:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click to select the server for which you want to inhibit replication.
3. Click **Inhibit Replication**.

   A confirmation box displays the message, **Inhibit replication to server <servername>. Are you sure?**

4. Click **OK**.

Replication for the selected server is inhibited. The text on the button changes from **Inhibit Replication** to **Allow Replication** for the selected server, and **Inhibited** appears in the last column in the selected server's row. When you are ready to allow replication on this server again, click **Allow Replication**.

Backing up data

Backup allows you to capture and archive data configured and/or provisioned on a specific NOAMP or SOAM server. All files that are part of the backup are archived into a single file in the file management storage area. For information on file storage and file name format conventions, see *Files*.

A backup of configuration and/or provisioning data on the NOAMP or on an SOAM server can be initiated or terminated from the **Database Status** page. The status of a backup can viewed from the **Backup and Archive** page.

Note: You must be logged into the active server to backup data for that server. For example, to perform a backup of NOAMP configuration or provisioning data, you must be logged into the active NOAMP. To perform a backup of SOAM configuration data, you must be logged into the active SOAM. Data backup is handled solely by NOAMP servers in systems that do not support SOAMs.

Note: Only Configuration data can be backed up on SOAM. The Provisioning button is not functional on SOAM and cannot be checked. Only the Configuration button is active.

Use this procedure to backup data for a server.

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click **Disable Provisioning**, then click **OK**.

   Provisioning and configuration updates are disabled for all servers, and the **Disable Provisioning** button changes to **Enable Provisioning**.

   Note: On an NOAMP, this means provisioning and configuration are disabled system-wide. On an SOAM, configuration is disabled only on the SO level.

3. Click to select the Active server in the Network Element that contains the data you want to backup.
4. Click **Backup**.

   The **Database Backup** page appears.

5. Select the data to be backed up, either **Provisioning**, **Configuration**, or both.

   Note: Only Configuration data can be backed up on SOAM. The Provisioning button is not functional on SOAM and cannot be checked. Only the Configuration button is active.

6. Select the backup archive compression algorithm, either gzip, bzip2, or none.

   Note: When backing up a database above 300M for SDS provisioning, it is recommended that you do not use bzip2.

7. Enter a comment in the **Comment** field to identify the backup file.

   This information is stored as part of the backup file and is displayed before a restore of the file occurs.

8. Change the **Archive Filename**, if desired.
9. Click **Ok**.

The backup begins. When the backup begins, the **Database Status** page appears again. The status of the backup appears in the information message box with a message similar to this:

```
Backup on <server_name> status MAINT_IN_PROGRESS.
```

The only action that can be taken for this server while a backup is in progress is **Report**. The backup is complete when the status message changes to:

```
Backup on <server_name> status MAINT_CMD_SUCCESS. Success
```

10. Click **Enable Provisioning**, then click **OK**.

    Note: You do not have to wait until the backup is complete to re-enable provisioning and configuration updates.

    Provisioning and configuration updates are enabled for all servers, and the **Enable Provisioning** button changes to **Disable Provisioning**.

The backed up data is stored in a compressed file and copied to the file management storage area of the server that was backed up. Use the **Status & Manage > Files** option to access this file. To transfer the file off-site, use the procedure, *Uploading a file to an alternate location*.

Database Archive Compare elements

The **Database Archive Compare** page displays a database report for the selected server. The databases and topologies are compared and the results displayed. This table describes the elements of the **Database Archive Compare** page.

Table 82: Database Status Elements

Element	Description
Archive Contents	The type of data that has been archived.
Database Compatibility	The compatibility status of the databases being compared.
Node Type Compatibility	The compatibility status of the relevant nodes.
Topology Compatibility	The compatibility status of the topology.
User Compatibility	The compatibility of the user and authentication data.
Contents	The contents of the archived database.
Table Instance Counts	Compares the number of database tables in the current database versus the database archive.

Comparing a backup file to an active database

The **Compare** page allows you to select a backup file in the file management storage area to compare and authenticate to the current database on the selected server. You must have at least two backup files in order to do a comparison.

Use this procedure to compare a backed up file with an active database:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click to select the server whose data you want to compare to a backup.
3. Click **Compare**.
4. The **Database Compare** page appears.
5. Click a radio button to select the backup to compare.
6. Click **OK**.

   The **Database Archive Compare** page appears displaying a database report for the selected server. The databases and topologies are compared and the results displayed.

7. Click **Print** to print the report.
8. Click **Save** to save the report to a file.

Restoring data to the active NOAMP server

CAUTION

Caution: This information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. The database restore operation is a service affecting procedure and careful consideration needs to be taken before executing database restore. All restore procedures shall be performed by Oracle Communications or its authorized representatives using the product specific Disaster Recovery guide.

Restore allows you to select and re-apply previously stored data across all components. Restorations can only be performed from the active NOAMP server.

Note: Restoration to any server other than the active NOAMP prevents proper provisioning and replication control within the network.

Restoration causes HA activity to switch from the targeted NOAMP server at the start to the mate of the target server, and back again on completion.

During restoration, the target server's database is stopped so that the database tables may be replaced with those contained in the Backup and Archive file. No alarms, events, measurements, or other stateful or collected data is archived by the target server for that time period. The target server begins recollecting that data once restoration is complete.

Restoration automatically enacts replication control on all application servers. This isolates the changes to the server being restored and allows the remainder of the network to operate without impact. Restoration automatically disables provisioning using the provisioning control subsystem. This stabilizes the database contents for the duration of the restoration procedure.

Several procedures are used during the restore process. The order in which they are performed varies depending on the number of servers and the setup of your system. Before data restoration can occur, the archived file being restored must be transferred to the file storage area . For more information, see *Uploading a local file*.

The documentation that came with your application provides a detailed list of all steps to perform during a restore, as well as the order in which to perform them. However, this information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. Contact My Oracle Support for more information about restoring data.

Confirming a restore procedure on the active NOAMP server

Caution: This information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. The database restore operation is a service affecting procedure and careful consideration needs to be taken before executing database restore. All restore procedures shall be performed by Oracle Communications or its authorized representatives using the product specific Disaster Recovery guide.

After the restore procedure is initiated, the **Database Restore Confirm** page appears. This page contains information about the compatibility status of the server and the selected archive.

The documentation that came with your application provides a detailed list of all steps to perform during a restore, as well as the order in which to perform them. However, this information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. Contact My Oracle Support for more information.

Replicating restored data to an SOAM server

When data is restored to the NOAMP, the data must be replicated to one SOAM server in each signaling network element, if the system supports SOAMs.

Caution: This information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. All restore procedures shall be performed by Oracle Communications or its authorized representatives.

This procedure describes the process used to replicate restored data to an SOAM server:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Locate all standby SOAM servers in the server table.
3. Click **Allow Replication** for each of these servers.

   Allow Replication displays for servers that are currently inhibited from receiving replicated database updates. This action enables replication for the selected servers. (For servers currently allowed to receive replicated database updates, the word **Inhibit Replication** displays here instead).

4. Select **Status & Manage > Replication**.

   The **Replication** page appears.

5. Verify that Auto Refresh is turned on.

   When the replication audit starts for a specific server, the Replication Status for that server displays **Not Replicating**, and Replication Channel Status displays **Audit**.

6. When the replication audit is complete, Replication Status returns to **Replicating** and Replication Channel Status returns to **Active**.
7. Select **Status & Manage > HA**.

   The **HA** page appears.

8. Switch over the high availability state of the standby SOAM servers.

For more information about setting the high availability state, see *HA (High Availability)*.

Replication is restored, and standby SOAM servers are updated with data from the restored backup. See *Replicating restored data to an MP server*, for information about how to manually turn replication back on for MP servers.

Replicating restored data to an MP server

When data is restored to SOAM servers, the data must be replicated to each MP server.

CAUTION

Caution: This information is provided for informational purposes only and does not grant permission to the customer to enact these procedures. All restore procedures shall be performed by Oracle Communications or its authorized representatives.

Use this procedure to replicate restored data to an MP server:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Locate all MP servers.
3. Click **Allow Replication** for each of these servers.

   Replication resumes for each of these servers.

4. Select **Status & Manage > Replication**.

   The **Replication** page appears.

5. Verify that Auto Refresh is turned on.
6. When the replication audit starts for a specific server, the Replication Status for that server displays **Not Replicating**, and Replication Channel Status displays **Audit**.
7. When the replication audit is complete, Replication Status returns to **Replicating** and Replication Channel Status returns to **Active**.
8. Select **Status & Manage > HA**.

   The **HA** page appears.

9. Switch over the high availability state of the standby MP servers.

   For more information about setting the high availability state, see *HA (High Availability)* .

Replication is restored on the selected servers, and the servers are updated with data from the restored backup.

Enabling and disabling provisioning on the active NOAMP server

Use this procedure to enable or disable provisioning updates on the active NOAMP server:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click **Enable Provisioning**.

Provisioning and configuration updates are enabled on all active NOAMP servers in the system. The **Enable Provisioning** button switches to **Disable Provisioning**.

3. To disable provisioning on a NOAMP GUI, click **Disable Provisioning**.

Enabling and disabling provisioning on the active SOAM server

Use this procedure to enable or disable provisioning updates on the active SOAM server:

1. Select **Status & Manage > Database**.

   The **Database Status** page appears.

2. Click **Enable Site Provisioning**.
   Provisioning and configuration updates are enabled on all active SOAMs at the SO level. The **Enable Site Provisioning** button switches to **Disable Site Provisioning**.
3. To disable provisioning on a SOAM GUI, click **Disable Site Provisioning**.

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server.

KPIs server elements

Table 83: KPIs Server Elements

KPIs Status Element	Description
Name	The KPI name.
Max	Maximum value of the KPI name within the selected scope.
Min	Minimum value of the KPI name within the selected scope.
Median	Median value of the KPI name within the selected scope.
Average	Average value of the KPI name within the selected scope.
Sum	Summary of all values of the KPI name within the selected scope.
Description	Description of the KPI name.

Viewing KPIs

Use this procedure to view KPI data.

1. Select **Status & Manage > KPIs**.

   The **Status & Manage KPIs** page appears with the **Server** tab displayed. For details about the KPIs displayed on this page, see the application documentation.

2. Click to select an application tab to see KPI data relevant to the application.

   Note: The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server. Collection of KPI data is handled solely by NOAMP servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the **KPIs Export** page.

Table 84: Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments

Element	Description	Data Input Notes
		Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the **KPIs** page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **KPIs** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to schedule a data export task.

1. Select **Status & Manage > KPIs**.

   The **KPIs** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The KPIs are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule KPI Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *KPIs data export elements* .
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

8. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

9. Click **OK** or **Apply** to initiate the KPI export task.

   From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*

- *Deleting a scheduled task*
- *Generating a scheduled task report*

Processes

The **Processes** page displays process status and other process information on a per-process basis for all servers in the system. Processes are controlled at the server level using the Stop, Restart, and Reboot options on the Servers page. See *Server* for more on Stop, Restart, and Reboot.

Process status elements

This table describes elements on the **Status & Manage Processes** page.

Table 85: Process Status Elements

Process Status Element	Description
Hostname	The hostname of the server.
Process Name	Name of the process, based on a unique identifying process tag within the application. Multiple processes on a server with the same name are appended with an instance number (#), for example, idbsvc(0) and idbsvc(1).
Start Time	Date and time the process was last (re)started.
Status	Status of the process. Possible values are: • **Up**: Process is up and running. Processes which are started successfully and reach a steady-state have a status of Up. • **Done**: The process is complete. • **Kill**: Process is being stopped. This is the normal state for a process to enter while being stopped. If a process is failing to shutdown, it remains in the Kill state for an extended amount of time. • **Pend**: Process execution is pending, waiting to be (re)started. Processes that have exited abnormally from the Up state shall fall into the Pend state. Processes that cannot start successfully shall remain in the Pend state. • **Unknown**: A failure is preventing the reporting or collection of the process status.
# Starts	Number of times the process started. All counts are 1 when a server boots up. The count increments to 2 if the process restarts and

Process Status Element	Description
	increments with each process restart. The count resets to 1 if the server is rebooted.
CPU Utilization	An estimate of recent CPU percentage used per process on the server.
Memory Used (%)	Percent of total memory used per process on the server.
Memory Used (Total) (K)	Total memory consumption per process including text, data, library, shared memory, etc., in Kilobytes.
Heap Memory Used (K)	Size of the heap used per process in Kilobytes.

Viewing Processes

Use this procedure to view all processes running on application servers:

Select **Status & Manage > Processes**.

The **Processes status** page appears. For more information about the fields displayed on the **Status & Manage > Processes** page, see *Process status elements* .

Tasks

The **Tasks** pages display the active, long running tasks and scheduled tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results for long running tasks, while the **Scheduled Task**s page provides a location to view, edit, and delete tasks that are scheduled to occur.

Active Tasks

The **Active Tasks** page displays the long running tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results, all of which can be generated into a report. Additionally, you can pause, restart, or delete tasks from this page.

Viewing active tasks

Use this procedure to view the active tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

All active tasks on the selected server are displayed.

Active Tasks elements

The **Active Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Active Tasks** page.

Table 86: Active Tasks Elements

Active Tasks Element	Description
ID	Task ID
Name	Task name
Status	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Start Time	Time and date when the task was started
Update Time	Time and date the task's status was last updated
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task
Progress	Current progress of the task

Deleting a task

Use this procedure to delete one or more tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the cursor over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

   Note: To delete a single task or multiple tasks, the status of each task selected must be one of the following: completed, exception, or trapped.

   Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold Ctrl as you click to select specific rows.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Deleting all completed tasks

Use this procedure to delete all completed tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the cursor over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Click **Delete all Completed**.
   A confirmation box appears.
4. Click **OK** to delete all completed tasks.
   All tasks with the status of completed are deleted.

Canceling a running or paused task

Use this procedure to cancel a task that is running or paused.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the cursor over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select a task.
4. Click **Cancel**.
   A confirmation box appears.
5. Click **OK** to cancel the selected task.
   The selected task is canceled.

Pausing a task

Use this procedure to pause a task.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select a task.

   Note: A task may be paused only if the status of the task is running.

4. Click **Pause**.
   A confirmation box appears.

5. Click **OK** to pause the selected task.
   The selected task is paused. For information about restarting a paused task, see *Restarting a task*.

Restarting a task

Use this procedure to restart a task.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select a paused task.

   Note: A task may be restarted only if the status of the task is paused.

4. Click **Restart**.
   A confirmation box appears.
5. Click **OK** to restart the selected task.
   The selected task is restarted.

Active Tasks report elements

The **Active Tasks Report** page displays report data for selected tasks. This table describes elements on the **Active Tasks Report** page.

Table 87: Active Tasks Report Elements

Active Tasks Report Element	Description
Task ID	Task ID
Display Name	Task name
Task State	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Admin State	Confirms task status
Start Time	Time and date when the task was started
Last Update Time	Time and date the task's status was last updated
Elapsed Time	Time to complete the task
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task

Generating an active task report

Use this procedure to generate an active task report.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

4. Click **Report**.
   The **Tasks Report** page appears.
5. Click **Print** to print the report.
6. Click **Save** to save the report.

Scheduled Tasks

The periodic export of certain data can be scheduled through the GUI. The **Scheduled Tasks** page provides you with a location to view, edit, delete and generate reports of these scheduled tasks. For more information about the types of data that can be exported, see:

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting security log files*
- *Exporting KPIs*
- *Exporting measurements reports*

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

Select **Status & Manage > Tasks > Scheduled Tasks**.

The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

Scheduled Tasks elements

The **Scheduled Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Scheduled Tasks** page.

Table 88: Scheduled Tasks Elements

Scheduled Tasks Element	Description
Task Name	Name given at the time of task creation
Description	Description of the task
Time of Day	The hour and minute the task is scheduled to run
Day-of-Week	Day of the week the task is scheduled to run
Network Elem	The Network Element associated with the task

Editing a scheduled task

Use this procedure to edit a scheduled task.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select a task.
3. Click **Edit**.
   The **Data Export** page for the selected task appears.
4. Edit the available fields as necessary.
   See *Scheduled Tasks elements* for details about the fields that appear on this page.
5. Click **OK** or **Apply** to submit the changes and return to the **Scheduled Tasks** page.

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.
3. Click **Delete**.
   A confirmation box appears.
4. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

3. Click **Report**.
   The **Scheduled Tasks Report** page appears.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

Files

The **Files** page provides access to the file management storage area of all servers configured on the system. This area is used to store and manage files generated by OAM server operations such as backup data and measurement processes. In addition to viewing and deleting files, you can also use the **Files** page to download existing files to an alternate location and upload new files.

File status elements

The **Files** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes the elements on the **Files** page.

Table 89: File Elements

Element	Description
File Name	Name of the file
Size	File size. Sizes are shown in one of the following units: PB (petabyte), TB (terabyte), GB (gigabyte), MB (megabyte), KB (kilobyte), or B (byte).
Type	File extension type
Timestamp	Time and date of file creation on the server

File name formats

This table describes the file name formats for files written to the file management storage area of the application. These variables are used in the file name formats:

- **<server name>** or **<hostname>** is the server hostname from which the file is generated.
- **<application name>** is the name of the application.
- **<groupname>** is the type of data stored in the backup file.
- **<NodeType>** specifies whether the backup was generated on an NOAMP or SOAM.
- **<time_date>** or **<YYYYMMDD_HHMMSS>** is the date and time that the file was generated.
- **(AUTO | MAN)** indicates whether the backup was automatically or manually generated.

Note: The file types listed here are among the most commonly seen in the file management storage area. The list, however, is not exhaustive and other file types may appear in the storage area.

Table 90: File Name Formats

File Type	File Name and Description
Backup	**Backup.<application name>.<hostname>.<groupname> [And<groupname>… [And <groupname>]] .<NodeType>.YYYYMMDD_HHMMSS.(AUTO | MAN).tbz2** A BZIP2 compressed tar file (tape archive format). This format can contain a collection of files in each tbz2 file. This file must be unzipped before it can be viewed.
Measurements	**Meas.<application name>.<server name>.<time_date>.csv** Comma-separated value file format used for storing tabular data. Measurement reports can be exported to the file management storage area, and are stored in csv format. See *Exporting measurements reports* for steps on exporting. Measurements reports generated from the SOAM GUI are limited to measurements for all MP and SOAM servers within that Network Element. A measurements report generated from an active SOAM server is identical to the one generated form a standby SOAM server since the measurements from the MPs are sent to and merged by both the SOAM servers within a Network Element. **Note:** Collection of Measurement data is handled by NOAMP servers in systems that do not support SOAMs.
Logs	**Logs.<application name>.<server name>.<time_date>.tgz** Log file. This is a g-zipped (GNU zip) tar file (tape archive format). This format can contain a collection of files in each tgz file. This file must be unzipped before it can be viewed.

Note: It is recommended that policies be developed to prevent overuse of the storage area. These might include a procedure to delete export files after transferring them to an alternate location, or removing backup files after a week, for example.

The Files option must have a check mark on the **Administration > Group** page for you to have access to the Files menu option.

Displaying the file list

Use this procedure to view the list of files located in the file management storage area of a server. The amount of storage space currently in use can also be viewed on the Files page.

1. From the Main menu, select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.

Viewing a file

Use this procedure to view, print, or save the contents of a file in the file management storage area.

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.
3. Select the file you want to view.

   Note: The **View** button is disabled when the contents of the file cannot be viewed from the GUI. For example, if a tar file is selected, the **View** button will be disabled, because the contents of tar files cannot be viewed from the GUI.

4. Click **View**.
   The contents of the file are displayed.
5. Click **Print** to print the file contents, or click **Save** to save the file.

Uploading a file to an alternate location

Use this procedure to move a file from the file management storage area to an alternate location.

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.
3. Select the file you want to move.
4. Click **Download**.
   Your browser's file download window appears.
5. Click **Save**.

   You browser's **Save As** window appears.

6. Navigate to the drive and folder where you want to save the file.
7. Click **Save**.

The file is saved to the specified location.

Uploading a local file

This procedure allows you to transfer a file from your local computer to the file management storage area of any server in the topology. A file up to 2 GB in size can be uploaded to the file management storage area.

Note: This product currently only supports file uploads and transfers for files less than 2 GB in size. To upload or transfer files greater than 2 GB in size, contact the My Oracle Support for assistance.

Use this procedure when you want to transfer a local file to the file management storage area:

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.
3. Click **Upload**.
   A dialog box appears.
4. Click **Browse** to select the file to upload.

   The **Choose File** window appears, allowing you to select a file to upload.

5. Select the file and click **Open**.

   The selected file and its path display in the file upload field.

   Note: Before proceeding, verify the selected file is uniquely named to avoid unintentionally overwriting another file.

6. Click **Upload**.

   A progress bar shows the status of the upload. When the upload is complete, an **Upload Complete** message appears.

   Note: Do not close the **Status & Manage Files** page during the upload. If you attempt to navigate away from the **Status & Manage Files** page during the upload, a dialog will appear to confirm the action. If the page is closed before upload completes, the transfer of data is stopped.

   The file is now stored in the selected server's file management storage area.

Deploying an ISO file

Use this procedure deploy an ISO file:

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select the ISO file.

3. Select**Deploy ISO**
   The ISO deploys to the server and is made available for upgrade on the server and all subtending servers. You can view the current deployment status using the Tasks drop down at the top left of the screen.

Deleting files from the file management storage area

If a Minor or Major Alarm is raised indicating either a minimum of 80% or 90% of file management space is used, old backup files can be deleted to clear space on that server.

Use this procedure remove one or more files from the file management storage area.

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.
3. Select the file you want to delete.
4. Click **Delete**.

   A **deletion confirmation** window appears.

5. Click **OK**.

   The file is deleted and space is cleared on the server.

6. Repeat this procedure for each file to be removed.

The deleted files are cleared from the server, and space becomes available in the file management storage area.

Chapter 8

Measurements

Topics:

This section provides an overview of the options on the **Measurements** page. All components of the system measure the amount and type of messages sent and received. Measurement data collected from all components of the system can be used for multiple purposes, including discerning traffic patterns and user behavior, traffic modeling, size traffic sensitive resources, and troubleshooting. This section provides an overview of measurements, describes how to generate and export a measurements report, and provides a list of register types.

Measurements

The measurements framework allows applications to define, update, and produce reports for various measurements.

- Measurements are ordinary counters that count occurrences of different events within the system, for example, the number of messages received. Measurement counters are also called pegs. Additional measurement types provided by the Platform framework are not used in this release.
- Applications simply peg (increment) measurements upon the occurrence of the event that needs to be measured.
- Measurements are collected and merged at the SOAM and NOAM servers as appropriate.
- The GUI allows reports to be generated from measurements.

Measurements that are being pegged locally are collected from shared memory and stored in a disk-backed database table every 5 minutes on all servers in the network. Measurements are collected every 5 minutes on a 5 minute boundary, i.e. at HH:00, HH:05, HH:10, HH:15, and so on. The collection frequency is set to 5 minutes to minimize the loss of measurement data in case of a server failure, and also to minimize the impact of measurements collection on system performance.

All servers in the network (NOAMP, SOAM, and MP servers) store a minimum of 8 hours of local measurements data. More than 5 minutes of local measurements data is retained on each server to minimize loss of measurements data in case of a network connection failure to the server merging measurements.

Measurements data older than the required retention period are deleted by the measurements framework.

Measurements are reported in groups. A measurements report group is a collection of measurement IDs. Each measurement report contains one measurement group. A measurement can be assigned to one or more existing or new measurement groups so that it is included in a measurement report. Assigning a measurement ID to a report group ensures that when you select a report group the same set of measurements is always included in the measurements report.

Note: Measurements from a server may be missing in a report if the server is down; the server is in overload; something in the Platform merging framework is not working; or the report is generated before data is available from the last collection period (there is a 25 to 30 second lag time in availability).

Measurement elements

This table describes the elements on the **Measurements Report** page.

Table 91: Measurements Elements

Element	Description	Data Input Notes
Scope	Network Elements, Server Groups, Resource Domains, Places and Place Associations for	Format: Pulldown list Range: Network Elements in the topology; Server Groups in the

Element	Description	Data Input Notes
	which the measurements report can be run. **Note:** Measurements for SOAM network elements are not available in systems that do not support SOAMs.	topology; Resource Domains in the topology; Places in the topology; Place Associations in the topology **Note:** If no selection is made, the default scope is Entire Network. Default: Entire Network
Report	A selection of reports	Format: Pulldown list Range: Varies depending on application Default: Group
Column Filter	The characteristics for filtering the column display	Format: Pulldown list Range: Sub-measurement Sub-measurement Ranges: • Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123. • In: A list-matching distinction for sub-measurement ID, for example, 3,4,6-10 matches only sub-measurements 3, 4, and 6 through 10. Default: None
Time Range	The interval of time for which the data is being reported, beginning or ending on a specified date.	Format: Pulldown list Range: Days, Hours, Minutes, Seconds Interval Reference Point: Ending, Beginning Default: Days

Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.

The **Measurements Report** page appears.

2. Select the **Scope**.
   For details about this field, or any field on the **Measurements Report** page, see *Measurement elements*
   .
3. Select the **Report**.
4. Select the **Interval**.
5. Select the **Time Range**.
6. Select **Beginning** or **Ending** as the **Time Range** interval reference point.
7. Select the **Beginning** or **Ending** date.
8. Click **Go**.
   The report is generated.

   Note: Data for the selected scope is displayed in the primary report page. Data for any available sub-scopes are displayed in tabs. For example, if the selected scope is Entire Network, report data for the entire network appears in the primary report page. The individual network entities within the entire network are considered sub-scopes.

9. To view report data for a specific sub-scope, click on the tab for that sub-scope.
   The report data appears.

Measurements data export elements

This table describes the elements on the **Measurements Report Export** page.

Table 92: Schedule Measurement Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily

Element	Description	Data Input Notes
		Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting measurements reports

You can schedule periodic exports of data from the **Measurements Report** page. Measurements data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied on the **Measurements Report** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to save a measurements report to the file management storage area.Use this procedure to schedule a data export task.

1. Select **Measurements > Report**.

   The **Measurements Report** page appears. For a description of each field, see *Measurement elements* .

2. Generate a measurements report.

   For information about how to generate a measurements report, see *Generating a measurements report*.

3. Click to select the scope or sub-scope measurement report that you want to export.
4. Click **Export**.

   The measurement report is exported to a CSV file. Click the link at the top of the page to go directly to the **Status & Manage** > **Files** page. From the **Status & Manage** page, you can view a list of files available for download, including the measurements report you exported during this procedure. The **Schedule Measurement Log Data Export** page appears.

5. Check the **Report Groups** boxes corresponding to any additional measurement reports to be exported.

   Note: This step is optional, but is available to allow the export of multiple measurement group reports simultaneously.

6. Select the **Export Frequency**.

   Note: If the selected **Export Frequency** is **Fifteen Minutes** or **Hourly**, specify the **Minutes.**

7. Enter the **Task Name**.
   For more information about Task Name, or any field on this page, see *Measurements data export elements* .

   Note: **Task Name** is not an option if **Export Frequency** equals **Once**.

8. Select the **Time of Day**.

   Note: **Time of Day** is only an option if **Export Frequency** equals **Daily** or **Weekly**.

9. Select the **Day of Week**.

   Note: **Day of Week** is only an option if **Export Frequency** equals **Weekly**.

10. Click **OK** or **Apply** to initiate the data export task.

    The data export task is scheduled. From the **Status & Manage** > **Tasks** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

    Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage** > **Tasks**. For more information see:

    - *Viewing scheduled tasks*
    - *Editing a scheduled task*
    - *Deleting a scheduled task*
    - *Generating a scheduled task report*

Glossary

A

AES	Advanced Encryption Standard
AVP	Attribute-Value Pair The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

C

CAPM	Computer-aided policy making
Charging Proxy Application	A DSR Application that is responsible for sending and receiving Diameter accounting messages.
ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
Communication Agent	See ComAgent.
CPA	Capability Point Code ANSI Charging Proxy Application - The Charging Proxy Application (CPA)

C

	feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

F

FABR	Full Address Based Resolution Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.
Full Address Based Resolution	See FABR.

G

GLA	Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by

G

	either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.
GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

I

IP	Intelligent Peripheral Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.
ISO	International Standards Organization

K

KPI	Key Performance Indicator

M

MP	Measurement Platform Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

N

NOAM	Network Operations, Administration, and Maintenance

O

OAM	Operations, Administration, and Maintenance The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.
OAM&P	Operations, Administration, Maintenance, and Provisioning. These functions are generally managed by individual applications and not managed by a platform management application, such as PM&C Operations – Monitoring the environment, detecting and determining faults, and alerting administrators. Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.

O

Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).

Provisioning – Setting up user accounts, devices, and services.

OAMP

Operations, Administration, Maintenance and Provisioning

R

RBAR

Range Based Address Resolution

A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing Entity" Type, and Routing Entity address ranges.

S

SBR

Subsystem Backup Routing

Session Binding Repository - A highly available, distributed database for storing Diameter session binding data

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol

S

	arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance Site Operations, Administration, and Maintenance

T

TSA	Target Set Address An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.