Oracle® Communications Tekelec Platform

Operations, Administration, and Maintenance (OAM)

Release 8.4

F12289-03

April 2021

ORACLE®

Oracle Communications Tekelec Platform Operations, Administration, and Maintenance (OAM), Release 8.4

F12289-03

Contents

3   Configuration

ORACLE®

4   Alarms and Events

5   Security Log

6   Status and Manage

ORACLE

7   Measurements

8   Common Security

List of Figures

List of Tables

1

Introduction

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.

Revision History

Date	Description
January 2016	Accessibility changes throughout.
August 2016	• Networking GUI and functionality updates, including Devices, Routes, and Services • Multiple Export feature added, including Filename Prefix and Task GUI elements • Active alarms export updates • Historical events data export elements and even history • Security log data and export updates • KPIs data export updates • Measurement data export updates
October 2016	General Options updates and GUI tabs for Entire Site selection
December 2016	• Automated Site Upgrade feature added • DSCP GUI and functionality updates
November 2020	Updated the range for Username element in the LDAP Authentication Elements section.
April 2021	Updated the Role for N/A in HA Status Elements section.

Overview

This documentation:

• Provides a conceptual overview of the application's purpose, architecture, and functionality

• Describes the pages and fields in 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 these 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 availability servers, databases, KPIs, processes, tasks, and files on the OAM.

- Measurements contains information on the measurement elements on the OAM.

My Oracle Support

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

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

1. Select **2** for New Service Request.

2. Select **3** for Hardware, Networking and Solaris Operating System Support.

3. Select one of the following options:

    - For Technical issues such as creating a new Service Request (SR), select **1**.

    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

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

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

2
Administration

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.

General Options

Use the General Options page to view a list of global options.

> **Note:**
>
> The General Options page content is dynamic and reflects parameters set in other code, and as such, there is no static number of rows in this page.

General Options Elements

Table 2-1 describes the elements of the General Options page.

Table 2-1   General Options Elements

Field (* indicates a required field)	Description	Data Input Notes
* Enable MMI Access	Enable Machine-to-Machine Interface access on servers. In addition to enabling the feature here, at least one user must be authorized for MMI access.	Format: Numeric Range: 0 (Disabled), 1 (Enabled) Default: 1
* Export File Compression Type	The compression algorithm used when export data files are initially created.	Format: Numeric Range: 0 (None), 1 (gzip), 2 (bzip2) Default: 1
* Last Login Expiration	Indicates the number of days of inactivity before a user account is disabled. The account is disabled the next time the user logs in using valid credentials. The account must be re-enabled by the guiadmin user or any user with admin group permissions. Entering a value of 0 indicates never disable.	Format: Numeric Range: 0 - 200 Default: 0

Table 2-1   (Cont.) General Options Elements

Field (* indicates a required field)	Description	Data Input Notes
* Lock out Window	Indicates the amount of time (in minutes) in which exceeding the **Maximum Consecutive Failed Login** attempts causes an account to be disabled. The account must be re-enabled by the guiadmin user or any user with admin group permissions. Entering a value of 0 indicates the window is unlimited and disables the **Maximum Consecutive Failed Login** attempts setting.	Format: Numeric Range: 0 - unlimited Default: 30
* Maximum Consecutive Failed Login	Indicates the maximum number of failed login attempts that can occur within the **Lock out window** before the account is disabled. The account must be re-enabled by the guiadmin user or any user with admin group permissions. Entering a value of 0 indicates never disable.	Format: Numeric Range: 0 - 10 Default: 5
* Maximum Password History	Maximum number of passwords maintained in a history list before reuse of a password is allowed. Entering a value of 0 in this field means that no password history is applied and the same password can be reused. A value is required.	Format: Numeric Range: 0 - 10 Default: 3
* Maximum Records per Page	The maximum number of records to display per page.	Format: Numeric Range: 10 - 100 Default: 20
* Minimum Password Difference	The Minimum character difference between passwords.	Format: Numeric Range: 0 - 16 Default: 0
* Minimum Password Length	This field indicates the minimum number of valid characters required for a user password.	Format: Numeric Range: 8 - 16 Default: 8

Table 2-1   (Cont.) General Options Elements

Field (* indicates a required field)	Description	Data Input Notes
* Password Expiration	The number of calendar days passwords stay active. By default, passwords expire in 90 days. Entering a value of 0 in this field means that passwords never expire. Note that the expiration is retroactive: if the expiration is set to 30 and it has been 45 days since the password was last changed, the password is now expired.	Format: Numeric Range: 0 - 90 Default: 90
* SAML Enabled	Enables SAML authentication of users (Security Assertion Markup Language).	Format: Numeric Range: 0 (Disabled), 1 (Enabled) Default: 0
* SAML Inactivity Timeout	The time (in minutes) before SAML authenticated sessions expire.	Format: Numeric Range: 0 (no expiration) - 3600 Default: 120
* Single Sign on Session Life	Indicates the maximum session life (in minutes) for a Single-Sign-On session.	Format: Numeric Range: 0 - 3600 Default: 120
* Site Upgrade Bulk Availability	Site based upgrade availability for bulk upgrade of MP groups. **Note**: This cannot be changed when any site upgrade is active.	Format: Numeric Range: 0 (none), 1 (50%), 2 (66%), and 3 (75%) Default: 1
* Site Upgrade SOAM Method	Site based upgrade SOAM method. **Note**: This cannot be changed when any site upgrade is active. Bulk upgrade will upgrade all non-active SOAM servers together.	Format: Numeric Range: 0 (serial), 1 (bulk) Default: 1
* Durability Administrative State	The durability state of the system.	Format: Numeric Range: 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 data is replicated to the active or standby NOs, as well as the secondary NO) Default: 1
Disabled Account	Message displayed when attempting to login to a disabled account.	Format: Alphabetic Default: This account has been disabled.

Table 2-1 (Cont.) General Options Elements

Field (* indicates a required field)	Description	Data Input Notes
Certificate Domain Name	Certificate Domain Name, used for Single Sign On and HTTPS certificates, for example, yourdomain.com.	Format: Alphanumeric, hyphen, and decimal characters Range: 255 characters Default: Blank
Failed Login Message	Message displayed on failed login.	Format: Alphabetic Default: Login failed
IP Authorization Denied Message	Configurable portion of IP Authorization Denied message.	Format: Alphabetic Default: Access denied
Login Message	Configurable portin of login message seen on the login screen.	Format: Alphabetic Default: Welcome to the Oracle System Login
Welcome Message	Welcome message seen after successful login. **Note**: You can customize the message appearance by using HTML code; for example, to insert a line break.	Format: Alphabetic Welcome message seen after successful login. The %loginName%, %lastLoginTime%, %loginAttempts%, and %lastLoginIP% tokens are replaced when the welcome message displays.
Export Data Space Replace	The character to replace a space in the export group name when added to the export directory or filename.	Format: Alphanumeric Default: Underscore (_)

Viewing the General Options Page

Use this procedure to view the general options page.

- Click **Administration**, and then **General Options**.

The **General Options** page lists all option variables, the current value of each variable, and a brief description of each setting including default values, if applicable.

Updating General Options

Use this procedure to update one or more general options.

You can change more than one option on this page.

1. Click **Administration**, and then **General Options**.
2. Locate the option or options you want to change in the variable column.
3. Change the value of the option or options.

   Input parameters are often provided in the description along with the default value if applicable.

4. Click **OK** to save the change(s) or **Cancel** to undo the change(s) and return the option(s) to the previously saved value(s).

The general option(s) are 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. The primary purpose of this page is to set up users for logging into the system. This page can also be used for adding users for the purpose of validating usernames and passwords in SOAP provisioning requests.

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.

System user

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**, and then **Options**. For more information, see General Options.

Insert New User Elements

Table 2-2 displays the following elements:

Table 2-2   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)

Table 2-2   (Cont.) User Administration Elements

Element	Description	Data Input Notes
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
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 Options	Select the ways users can access their account. The two options are Machine-to-Machine and GUI access. Both may be selected.	Format: Checkbox Range: Allow GUI Access and/or Allow MMI Access Default: GUI and MMI access enabled
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:**
>
> Before 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 before adding the user (see Add a Group).

Use this procedure to add a new user to the system.

> **✎ Note:**
>
> When setting up a user for SOAP provisioning request validation, the only field other than **Username** and **Group** used for this validation process is **Access Options**.

1. Click **Administration**, and then **Access Control**, and then **Users**.

2. Click **Insert**.

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 the **Access Options** allowed for this account. When setting up a user for SOAP provisioning request validation, check mark *Allow MMI Access*. It is highly recommended you also uncheck *Allow GUI Access* (users set up for SOAP request validation should not have UDR GUI access).

7. Select whether the account is enabled using the **Access Allowed** checkbox.

8. Enter the **Maximum Concurrent Logins**.

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

9. Enter the **Session Inactivity Limit**.

10. Enter text about this user in the **Comment** field.

    This field is required.

11. Perform one of the following actions:

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

    • Click **OK**.
      The Users administration page displays again with the new user displayed.

    The new user is added to the database.

User Administration Elements

Table 2-3 displays the following elements.

Table 2-3   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	Remote authorization is enabled or disabled.
Local Auth	Local authorization is enabled or disabled.
GUI Access	GUI access is enabled or disabled.
MMI Access	Machine-to-Machine Interface access 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 list of 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. Click **Administration**, and then **Access Control**, and then **Users**.

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

2. To view more detailed information, select a user and click **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. Click **Administration**, and then **Access Control**, and then **Users**.

2. Select a user from the listing.

3. Click **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 does 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. Click **Administration**, and then **Access Control**, and then **Users**.

2. Select the appropriate user from the listing.

3. Click **Delete**.

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

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. Click **Administration**, and then **Access Control**, and then **Users**.

2. Select a **Username** from the listing.

3. Click **Edit**.

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 Group 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 does not affect the user's current session.

1. Click **Administration**, and then **Access Control**, and then **Users**.

2. Select the appropriate user from the listing.

3. Click **Edit**.

4. Select the appropriate groups from the **Group** listing.

5. Click **OK**.

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

Generating a User Report

A user account usage report can be generated from the users 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. Click **Administration**, and then **Access Control**, and then **Users**.

2. Select one or more users.

> **Note:**
>
> If no users are selected, then all users appear in the users report.

3. Click **Report**.

   The Users 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.

Policy DRA Group Administration Permissions

Table 2-4 and Table 2-5 describe the Policy DRA Group Administration permissions.

The **Administration**, and then **Group** GUI page displays permissions checkboxes for all Policy DRA pages for both NOAM and SOAM.

• All of the permissions can be updated only on the NOAM **Administration**, and then **Group** page.

• All of the permissions can be viewed but not updated on the SOAM **Administration**, and then **Group** page.

Table 2-4   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 Clients 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

Table 2-4   (Cont.) Policy DRA Configuration Permissions

Permission	Description
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 2-5   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

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. Click **Administration**, and then **Access Control**, and then **Users**.
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 the values entered in both fields match.
5. Click **Continue**.
6. Click **Administration**, and then **Users** to return to the User Administration page.

The password has been updated in the database and takes 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 the **Change password** checkbox on the System Login page.
2. Enter the user name and password.
3. Click **Login**.

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

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

5. Click **Continue**.

   The password has been updated in the database, which takes 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. Click **Administration**, and then **General Options**.

2. Locate **Password Expiration** 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 does not prevent groups and users from being set up. Figure 2-1 displays these sections of the Group Administration page.

> **✎ Note:**
>
> When setting up users for SOAP provisioning request validation, it is recommended a separate non-administrative group be set up for these users.

Figure 2-1   Global Action and Administration Permissions

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

These checkboxes 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 checkboxes 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** checkbox 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 user account and group shown in Table 2-6 are delivered with the system and cannot be deleted or modified.

Table 2-6   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

Table 2-7 describes the OAM groups administration permissions.

Table 2-7   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	
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.

ORACLE®

Table 2-7   (Cont.) OAM Groups Administration Permissions

Permission	Description
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 Authentication.
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.
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 and 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.
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	

Table 2-7   (Cont.) OAM Groups Administration Permissions

Permission	Description
Report	Grants permission to create and export measurement reports.

IPFE Group Administration Permissions

Table 2-8 describes the IP Front End (IPFE) Group Administration permissions.

Table 2-8   IPFE Configuration Permissions

Permission	Description
Options	Allows a user to set up data replication between IPFEs, specify port ranges for TCP traffic and set application server monitoring parameters.
Target Sets	Allows a user to create, edit, view, and delete Target Sets and IP List TSAs.

Communication Agent Group Administration Permissions

Table 2-9 and Table 2-10 describe the Communication Agent (ComAgent) Group Administration permissions.

Table 2-9   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 2-10   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
Show HA Services Status	Allows a user to display **HA** Services Status

Diameter AVP Dictionary Group Administration Permissions

This section describes the Diameter AVP Dictionary Group Administration permissions.

Table 2-11   Diameter AVP Dictionary Group Administration Permissions

Permission	Description
AVP Dictionary	Allows a user to view, create, edit, delete, and manage AVP Dictionary
Vendors	Allows a user to view, create, edit, delete, and manage Vendors

DSR Diameter Group Administration Permissions

Table 2-12, Table 2-13, Table 2-14, and Table 2-15 describe the DSR Diameter Group Administration permissions:

Table 2-12   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.

Table 2-12   (Cont.) Diameter Configuration Permissions

Permission	Description
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.
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 2-13   Diameter Maintenance Permissions

Permission	Description
Route Lists	Allows a user to view priority, capacity, Route Group assignment, and status information for Route Lists.

ORACLE®

Table 2-13   (Cont.) Diameter Maintenance Permissions

Permission	Description
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.
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 2-14   Diameter Mediation Permissions

Permission	Description
Rule Templates	Allows a user to define Mediation Rule Templates.
Enumerations	Allows a user to view and edit Mediation Enumerations.
Triggers	Allows a user to view and edit Mediation Triggers.
State & Properties	Allows a user to set the state of a Rule Template and configure settings for a Rule Template.
Internal Variables	Allows the user to view, create, edit, and delete Interval Variables.
Measurements	Allows the user to view, create, edit and delete custom measurements and measurements based on a particular Action.
Rule Sets	Allows a user to define Mediation Rule Sets.

Table 2-15   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.

EIR Configuration Group Administration Permissions

This section describes the EIR Configuration Group Administration permissions.

Table 2-16   EIR Configuration Group Administration Permissions

Permission	Description
EIR Options	Allows a user to view and edit EIR Options
EIR Imsi Ranges	Allows a user to view, create, edit, and delete EIR Imsi Ranges

Radius Configuration Group Administration Permissions

This section describes the Radius Configuration Group Administration permissions.

Table 2-17   Radius Configuration Group Administration Permissions

Permission	Description
Ingress Status Server Cfg Set	Allows a user to view, create, edit, and delete Ingress Status Server Cfg Set
Message Authenticator	Allows a user to view, create, edit, and delete Message Authenticator
Shared Secret Cfg Set	Allows a user to view, create, edit, and delete Shared Secret Cfg Set
NAS Node	Allows a user to view, create, edit, and delete NAS Node
Network Options	Allows a user to view and edit Network Options
Message Conversion Cfg Set	Allows a user to view Message Conversion Cfg Set

RBAR Group Administration Permissions

Table 2-18 describes the Range-Based Address Resolution (RBAR) Group Administration permissions.

Table 2-18   RBAR Configuration Permissions

Permission	Description
Applications	Allows a user to create, view, and delete Applications
Exceptions	Allows a user to edit and view Exceptions
Destinations	Allows a user to create, edit, view and delete Destinations
Address Tables	Allows a user to create, view, and delete Address Tables
Addresses	Allows a user to create, edit, view, and delete Addresses

Table 2-18   (Cont.) RBAR Configuration Permissions

Permission	Description
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

SCEF Configuration Group Administration Permissions

This section describes the DSR Service Capability Exposure Function (SCEF) Configuration Group Administration permissions.

Table 2-19   SCEF Configuration Group Administration Permissions

Permission	Description
Nidd Configuration Sets	Allows a user to view, create, edit, and delete Nidd Configuration Sets
Apn Configuration Sets	Allows a user to view, create, edit, and delete Apn Configuration Sets
Monitoring Event Configuration Sets	Allows a user to view, create, edit, and delete Monitoring Event Configuration Sets
SCS Application Servers	Allows a user to view, create, edit, and delete SCS Application Servers
System Options	Allows a user to view and edit System Options
Device Triggering Configuration Sets	Allows a user to view, create, edit, and delete Device Triggering Configuration Sets
Access Control Lists	Allows a user to view, create, and delete Access Control Lists
Access Control Rules	Allows a user to view, create, edit, and delete Access Control Rules
Access Control Associations	Allows a user to view, create, and delete Access Control Associations

Service Broker Group Administration Permissions

Table 2-20 describes elements of the Group Administration page.

Table 2-20   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

FABR Group Administration permissions

Table 2-21 describes the Full Address-Based Resolution (**FABR**) Group Administration permissions.

Table 2-21   FABR Configuration Permissions

Permission	Description
Applications	Allows a user to create, view, and delete Applications.
Exceptions	Allows a user to edit and view 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 FABR System Options.

SSR Group Administration Permissions

Table 2-22, Table 2-23, Table 2-24, Table 2-25, and Table 2-26 describe the SSR group administration permissions.

Table 2-22   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 2-23   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.

Table 2-23   (Cont.) SSR Routing Permissions

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

Table 2-24   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 2-25   SIP Timer Permissions

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

Table 2-26   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.

Table 2-26 (Cont.) SSR Maintenance Permissions

Permission	Description
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

Table 2-27, Table 2-28, and Table 2-29 describe 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 2-27 SS7/Sigtran Configuration Permissions

Permission	Description
Adjacent Server Groups	Allows the user to view, insert, edit, and delete Adjacent Server Groups.
Local Signaling Points	Allows the user to view, insert, edit, delete, and generate a report on Local Signaling Points.
Remote Signaling Points	Allows the user to view, insert, delete, generate a report, and view status on Remote Signaling Points.
Remote MTP3 Users	Allows the user to view, insert, delete, and view the status of Remote MTP3 Users.
Link Sets	Allows the user to view, insert, delete, generate a report, and view status of Link Sets.
Links	Allows the user to view, insert, delete, generate a report, and view status of a Link.
Routes	Allows the user to view, insert, edit, delete, generate a report, and view status of Routes.
SCCP Options	Allows the user to view and edit SCCP Options.
MTP3 Options	Allows the user to view and edit MTP3 Options.
M3UA Options	Allows the user to view and edit MTP3 Options.
Local Congestion Options	Allows the user to view Local Congestion Options.
Local SCCP Users	Allows the user to view, insert, delete, generate a report, and view status of the Local SCCP Users.

Table 2-28   SS7/Sigtran Maintenance Permissions

Permission	Description
Local SCCP Users	Allows the user to view the status of Local SCCP Users and to enable and disable LSUs.
Remote Signaling Points	Allows the user to view the status of Remote Signaling Points and to reset the network status of routes.
Remote MTP3 Users	Allows the user to view the status of Remote MTP3 Users and to reset the subsystem and point code status.
Link Sets	Allows the user to view the status of Link Sets.
Links	Allows the user to view the status of Links and to enable and disable Links.
Associations	Allows the user to view the status of Associations and to enable, disable, and block Associations.

Table 2-29   SS7/Sigtran Command Line Interface

Permission	Description
Command Import	Allows the user to use the Command Import page.

Transport Manager Configuration Group Administration Permissions

This section describes the Transport Manager Group Administration permissions.

Table 2-30   Transport Manager Configuration Group Administration Permissions

Permission	Description
Adjacent Node	Allows a user to view, create, and delete Adjacent Node
Configuration Sets	Allows a user to view, create, edit, and delete Configuration Sets
Transport	Allows a user to view, create, edit, and delete Transport

Table 2-31   Transport Manager Maintenance Group Administration Permissions

Permission	Description
Transport	Allows a user to view and manage Transport

UDR Group Administration Permissions

Table 2-32 describes the UDR Group Administration permissions.

Table 2-32   UDR Group Administration Permissions

Permission Group	Description
UDR Configuration	
Provisioning Options	Allows a user to view and edit provisioning option settings.
Ud Client Options	Allows a user to view and edit Ud client option settings.
UDRBE Options	Allows a user to view and edit UDRBE option settings.
Ud Remote Server Configuration	Allows a user to view and edit Ud remote server configuration settings.
Provisioning Connections	Allows a user to view, add, edit, or delete provisioning connections.
Ud Client Key Details	Allows a user to view and edit Ud client key detail settings.
Subscribing Client Permissions	Allows a user to view, add, or delete subscribing client permissions.
Ud Client Attribute MAP SEC	Allows a user to view, add, edit, or delete Ud client attribute MAP SEC settings.
Subscriber Query and Provisioning	Allows a user to view, add, edit, or delete subscriber query and provisioning settings.
Create Profile/Add Entity	Allows a user to view and add profiles and entities.
Auto Enrollment Options	Allows a user to view and edit auto enrollment option settings.
Auto Enrollment Blacklist	Allows a user to view, add, or delete auto enrollment blacklist entries.
Command Log Export Options	Allows a user to view and edit command log export option settings.
Pool Spanning Options	Allows a user to view and edit Pool Spanning Option settings.
Pool Network Configuration	Allows a user to view, add, or delete pool network configurations.
UDR Key Range	Allows a user to view, add, or delete key ranges.
Ud Client Options	Allows a user to view and edit ud client option settings.
Ud Client Remote Server Configuration	Allows a user to view and edit ud remote server configuration settings.
Ud Client Attribute Mapping	Allows a user to view and edit ud attribute mapping.
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.

Table 2-32   (Cont.) UDR Group Administration Permissions

Permission Group	Description
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	Allows a user to view command log history.
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 Availability	Allows a user to view the status of subscribing clients.
Quota Reset Scheduler Tasks	Allows a user to view, add, edit, delete, or manage quota reset scheduler tasks.
Database Auditor	Allows a user to view and manage the database auditor.
Command Log Export Status	Allows a user to view the status of log exports.
Ud Client Connection Status	Allows a user to view, edit, or manage the status of ud client connections.

vSTP Configuration Group Administration Permissions

This section describes the vSTP Configuration Group Administration permissions.

Table 2-33   vSTP Configuration Group Administration Permissions

Permission	Description
Remote Hosts	Allows a user to view, create, edit, and delete Remote Hosts
Local Hosts	Allows a user to view, create, edit, and delete Local Hosts
vSTP Connections	Allows a user to view, create, edit, and delete vSTP Connections
vSTP Connection Status	Allows a user to view, edit, and manage vSTP Connection Status
vSTP Connection Configuration Sets	Allows a user to view, create, edit, and delete vSTP Connection Configuration Sets
vSTP Remote Signaling Points	Allows a user to view, create, edit, and delete vSTP Remote Signaling Points
vSTP Local Signaling Points	Allows a user to view, create, edit, and delete vSTP Local Signaling Points
vSTP Link Sets	Allows a user to view, create, edit, and delete vSTP Link Sets
vSTP Links	Allows a user to view, create, edit, and delete vSTP Links
vSTP Routes	Allows a user to view, create, edit, and delete vSTP Routes
vSTP Link Status	Allows a user to view, edit, and manage vSTP Link Status
vSTP Link Set Status	Allows a user to view, edit, and manage vSTP Link Set Status
vSTP Remote Signaling Point Status	Allows a user to view, edit, and manage vSTP Remote Signaling Point Status

Table 2-33   (Cont.) vSTP Configuration Group Administration Permissions

Permission	Description
vSTP Global Title Addresses	Allows a user to view, create, edit, and delete vSTP Global Title Addresses
vSTP GTT Sets	Allows a user to view, create, edit, and delete vSTP GTT Sets
vSTP GTT Selectors	Allows a user to view, create, edit, and delete vSTP GTT Selectors
vSTP Feature Admin States	Allows a user to view, create, edit, and delete vSTP Feature Admin States
vSTP Sccp Options	Allows a user to view and edit vSTP Sccp Options
vSTP MRN Sets	Allows a user to view, create, edit, and delete vSTP MRN Sets
vSTP MAP Sets	Allows a user to view, create, edit, and delete vSTP MAP Sets
vSTP M2pa Options	Allows a user to view and edit vSTP M2pa Options
vSTP M3rl Options	Allows a user to view and edit vSTP M3rl Options
vSTP MP Leader	Allows a user to view vSTP MP Leader
vSTP GTT Actions	Allows a user to view, create, edit, and delete vSTP GTT Actions
vSTP GTT Actions Sets	Allows a user to view, create, edit, and delete vSTP GTT Actions Sets
vSTP Capacity	Allows a user to view vSTP Capacity
vSTP MP Peers Status	Allows a user to view vSTP MP Peers Status
vSTP Alarm Aggregation Options	Allows a user to view and edit vSTP Alarm Aggregation Options

Add a Group

Use this procedure to add a new group:

1. Click **Administration**, and then **Access Control**, and then **Groups**.

2. Click **Insert**.

3. Enter a unique name in the **New Group Name** field, and optionally, in the **Description** field, enter text to describe the group. When setting up a group for the purpose of SOAP request validation, use a name to easily identify this purpose, such as SOAP Users.

4. To allow View, Insert, Edit, Delete or Manage actions on all pages accessed from the GUI, selectively check mark each action in the **Global Action Permissions** row.

   Checks appear next to each page under that action.

5. Check mark the remaining menu permissions to which you want this group to have access.

   > **Note:**
   >
   > For a group created for SOAP request validation, no permissions need to be check marked.

> **✎ Note:**
>
> To quickly select all permissions in a given section, place a check beside the desired section under the desired action. For example, if the group needs only view access for the **Alarms and Events** section, place a single check next to **Alarms and Events Permissions** and under the **View** action. For more information on the options displayed on the Group page, see Groups Administration.

6. Perform one of the following actions:

   - Click **Apply**.
     A confirmation message appears at the top of the Add Groups page to inform you that the new group has been added to the database. To close the Add Groups page, click **Cancel**.

   - Click **OK**.

   > **✎ 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 Insert New User Elements for more information.

The new group is added to the database.

Modify a Group

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

Use this procedure to modify a group:

1. Click **Administration**, and then **Access Control**, and then **Groups**.

2. Select the desired group from the Groups administration page.

3. Click **Edit**. For information on permission options, see OAM Groups Administration Permissions.

4. Modify the group permissions as needed.

   For information on permission options, see OAM Groups Administration Permissions.

5. Click **OK** or **Apply**.

   Clicking **OK** returns you to the Groups administration page and clicking **Apply** leaves you in the Groups edit page, but applies the changes.

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.

Delete a Group

> **Note:**
>
> The system does not allow any user to delete a predefined group provided during installation. See Pre-defined User and Group for more information on this topic.

Use this procedure to delete a group:

1. Click **Administration**, and then **Access Groups**, and then **Groups**.

2. Select the desired group from the Groups administration page and take note of any users presented in the **Users** pane.

> **Note:**
>
> The **Users** pane lists all users associated with the group. If there are users associated with the group, you must delete the users or assign them to another group before deleting the group. See Changing a User's Assigned Group.

3. Once all users have been cleared from the **Users** pane click **Delete**.

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

   A status box displays the results of the action.

   The group is removed from the database.

Generate a Group Report

A group report can be generated from the Groups administration page. This type of report provides information about a groups global action and administrative permissions.

1. Click **Administration**, and then **Access Control**, and then **Groups**.

2. Select one or more groups.

> **Note:**
>
> If no groups are selected then all groups appear in the group report.

3. Click **Report**.

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

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

Table 2-34 describes elements of the Sessions Administration page.

Table 2-34   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 expires.
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.

Deleting user sessions

Use this procedure to delete a user session.

> **Note:**
>
> You cannot delete your own session.

1. Click **Administration**, and then **Access Control**, and then **Sessions**.

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

    To distinguish the appropriate session, locate either the User or the IP address found in the corresponding pane. For more information 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
- TLS/DTLS over TCP/SCTP Transport - allows transport layer security protocols and encryption on a per connection basis at the application layer. For example, DSR local and peer node connections
- Single Sign-On (SSO) - allows users to navigate among several applications without having to re-enter login credentials
- Certificate Authority (CA) - A digital certificate provided by a trusted source used to make secure connections between a client and server.

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 DNS Configuration.

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

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 Element

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 Element

Table 2-35 describes the element used when configuring single sign-on zones.

Table 2-35   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. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

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

3. Enter a **Zone Name** that consists of 1-15 characters.

4. Click **Apply** to save the changes you have made and remain on this screen, or click **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 have to re-distribute the certificate for this zone to all the other remote zones 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. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select the local zone from the listing.

3. Click **Reestablish Local Zone**.

A confirmation message appears stating that re-establishing a local zone invalidates configured SSO key-exchanges involving this machine.

4. Click **OK**.

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. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select the appropriate zone from the table listing.

3. Click **Delete**.

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. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Click to select the zone for which you want to create a report.

> **✎ Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.

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 is included in your certificate such as your organization name, common name (domain name), locality, and country.

Create CSR Elements

Table 2-36 describes the elements used when creating a CSR.

Table 2-36   Create CSR Elements

Element	Description	Data Input Notes
Country	The 2-letter country code where the entity being described lives.	Range: A to Z
State or Province	The state or province (full name) where the entity being described lives.	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens.
Locality	The locality name (for example, city) of the entity being described.	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens.

Table 2-36   (Cont.) Create CSR Elements

Element	Description	Data Input Notes
Common Name	The common name of the entity being described. Replacing a certificate marked visible or active results in browser connection errors, which may require a reload or restart of the browser to restore connectivity. The list includes only those entities that do not already have an associated certificate.	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens.

Note:

Common Names are case insensitive and must be u

Table 2-36   (Cont.) Create CSR Elements

Element	Description	Data Input Notes
		nique.
Organization	The name of the organization to which the entity belongs.	Range: 1-100 character long string. Allowed characters are A-Z, a-z, spaces, and hyphens.
Organizational Unit	The organizational unit name (for example, section) to which the entity belongs.	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, . (period), and @ (at symbol)

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 to apply for a digital identity certificate.

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Click **Create CSR**.

3. Select a two-character **Country** code for the entity.

    For more information about any field on this page, see Table 2-36.

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.

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.

> **Note:**
>
> The maximum number of allowed TLS/DTLS certificates is 1000.

Import Certificate elements

Table 2-37 describes the elements used when importing a certificate.

Table 2-37   Import Certificate Elements

Element	Description	Data Input Notes
X.509 Certificate	PEM encoded X.509 certificate	Range: 2048 characters **Note**: For SSL (TLS/DTLS) certificates, valid range is 1024-2048 characters
Private Key	PEM encoded Private Key	Range: 2048 characters **Note**: For SSL (TLS/DTLS) keys, valid range is 1024-2048 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. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Click **Import**.

3. Enter the **X.509 Certificate**.

   For more information about any field on this page, see Table 2-37.

4. Enter the **Private Key**.

5. Enter the **Passphrase**.

6. Click **OK** to import the certificate.

Bulk Importing of Certificates

The following steps outline the procedures necessary to bulk import certificates by uploading a valid XML certificates file from a local workstation.

> **✎ Note:**
>
> The maximum allowed TLS/DTLS certificates is 1000. Attempting to import more than 1000 TLS/DTLS certificates, including existing certificates, results in an error message.

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Click **Browse**.

3. Navigate to the location of the XML certificates file on the local workstation. Select the file and click **Open**.

    The browsers upload window clears and the file name is presented next to the **Browse** button.

4. Click **Upload File**.

    During the upload process, checks are performed to verify a valid file extension and whether there is invalid data in the XML file being uploaded.

Updating a Certificate

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

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select the appropriate certificate from the table list.

3. Click **Update**.

4. Update the **X.509 Certificate**.

5. Click **OK** to update the certificate.

Deleting a Certificate

Use this procedure to delete a certificate:

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select the appropriate certificate from the table listing.

3. Click **Delete**.

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

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

Exporting Certificates

The following steps outline the procedures necessary to export certificates.

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select one or more certificates for export.

If no certificates are selected then all of the configured certificates shall be exported.

3. Click **Export**.

4. Select the appropriate action presented in the Open File screen.

   Depending on the action selected, the file opens in the preferred application or be saved to the local workstation.

Generate a Certificate Report

Use this procedure to generate a certificate report:

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Click to select the certificate for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.

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

Table 2-38 describes the elements on the **Authorized IPs** page.

Table 2-38   Authorized IPs Elements

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. Click **Administration**, and then **Access Control**, and then **Authorized IPs**.

   > **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.

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. Click **Administration**, and then **Access Control**, and then **Authorized IPs**.
2. Select the Info box in the upper left corner of the screen and click **Disable**.

Inserting Authorized IP Addresses

Use this procedure to insert authorized IP addresses.

> **Note:**
>
> This procedure pertains to GUI access only.

1. Click **Administration**, and then **Access Control**, and then **Authorized IPs**.
2. Click **Insert**.
3. Enter an IP address in the **IP Address Value** field.
4. Optional: Enter a comment in the **Comment Value** field.

ORACLE

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. Click **Administration**, and then **Access Control**, and then **Authorized IPs**.

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 lose access to the GUI. If this happens, contact the Customer Care Center.

3. Click **Delete**.

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 provides restricted access through those accounts to the export area of the file management directory to use for exporting MEAL data.

SFTP User elements

Table 2-39 describes the elements on the SFTP Users page.

Table 2-39   SFTP User elements

Element	Description
Username	The SFTP user name account.
	Range = Lowercase alphanumeric (a-z, 0-9) string between 5 and 32 characters long.

Table 2-39   (Cont.) SFTP User elements

Element	Description
Permissions	The permissions associated with the account. The user can 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. Click **Administration**, and then **Access Control**, and then **SFTP**.

2. Click **insert**.

3. Enter a **Username** to be used to identify the SFTP User.

   For more information about any field on this page, see Table 2-39.

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 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.

Updating SFTP User information

Use this procedure to update SFTP user information:

1. Click **Administration**, and then **Access Control**, and then **SFTP Users**.

2. Select the appropriate user from the listing.

3. Click **Edit**.

4. Make the desired updates to the user information.

5. 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. Click **Administration**, and then **Access Control**, and then **SFTP**.

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. Click **Administration**, and then **Access Control**, and then **SFTP**.

2. Select the appropriate user name from the listing for the SFTP user to delete.

3. Click **Delete**.

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

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. Click **Administration**, and then **Access Control**, and then **SFTP**.

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.

Updating SFTP User password settings

Use this procedure to update SFTP user password settings:

1. Click **Administration**, and then **Access Control**, and then **SFTP**.

2. Select the appropriate user from the listing and click **Change Password**.

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. Click **Continue**.

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. Click **Administration**, and then **Software Management**, and then **Versions**.
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.

Upgrade

The **Upgrade** menu choice is only available on the NOAM. It includes server, Server Group (SG) and Entire Site (ES) options. in this context, site refers to this grouping (SO SG plus all replication children MP SGs). This additional automation prevents having to initiate a server group upgrade on the SO group followed by additional form submissions for each MP group.

> **✎ Note:**
>
> In this context, site refers to the topological grouping of the SO SG and all its replication children MP SGs, regardless of geographic location of the servers. For example, the site upgrade includes a spare SOAM which is a member of SO SG, but is in another geographic location.

Use the Upgrade page to perform software upgrades and related functions on in-service servers in a network. In addition to initiating and accepting upgrades, this page provides to ability to perform backups, health checks (checkups), and reporting. Upgrade functionality is available on a server, SG, or site basis and supports pause, restart, and cancellation functionality.

There are several situations where the SG or site upgrade task automatically pauses or stops itself to allow you to perform recovery actions. You can then restart or cancel the overall upgrade. It is also possible to restart SG or site upgrade on a partially upgraded SG or site. When an SG or Site upgrade is paused or canceled, any currently running upgrades (from a TPD standpoint) continue until they complete or fail. Servers that are in the Pending state are not started.

SG upgrades automatically pause in the following situations:

- A server upgrade fails.

- A response of false from *canServerUpgrade()* function is received when the server requires an upgrade pre-check.

- A server upgrade is cancelled after being hung.

A SG upgrade can be ended by cancelling the SG upgrade from the **Status & Manage**, and then **Tasks**, and then **Active Tasks** page. The SG upgrade can then be restarted using the **Administration**, and then **Software Management**, and then **Upgrade** page. A site upgrade can be ended by cancelling the site upgrade from the **Status & Manage**, and then **Tasks**, and then **Active Tasks** page. The site upgrade can then be restarted using the **Administration**, and then **Software Management**, and then **Upgrade** page.

The server group upgrade provides the ability to upgrade all servers in a server group by filling out a form with options such as Mode and Availability, selecting an ISO, and clicking **OK** to initiate the upgrades. From that point, long running tasks on the NOAMP manage the upgrade of each server in the group, ensuring that enough servers in the group remain active to handle ongoing system management and subscriber traffic. While the servers are upgrading, you can view the progress of each server's upgrade. You can start an automated server group upgrade on multiple server groups with additional GUI actions.

> **Note:**
>
> The instructions in this section provide a generic framework for upgrades. You should always defer to the application specific upgrade instructions based on each release.

> **Caution:**
>
> We recommend you contact My Oracle Support and inform them of your upgrade plans before beginning this or any upgrade procedure. Before upgrading, go to the My Oracle Support website to acquire the correct upgrade procedure for your product and review any relevant Technical Service Bulletins (TSBs).

Upgrade Elements

Table 2-40 describes the elements on the Upgrade page. This page supports Automated Site Upgrade, as well as Automated Server Group (ASG) and server upgrade.

> **Note:**
>
> There can be two tabs on this page (the following tab labels are just examples): **NO_SG** and **SO_SGx**. The elements in Table 2-40 list all elements on both tabs. Only tabs with servers after filtering is applied are displayed. The SOAM server groups indicate which sites are eligible for site upgrade. **Entire Site** is only available on the **SO_SGx** tab.

The grid reflects the following rules:

- One row of tabs or two rows of tabs is displayed, depending on the selected server group.

- The top (or only) row is always the OAM server groups (NO and SO). Multiple NO and SO server group tabs can exist in the top row.

- The second row displays when an SO group is selected, and it contains an **Entire Site** tab, plus a tab for each SO and MP server group in the SO group's administrative domain. An administrative domain is a server group and its replication children SGs, which all share a topological relationship regardless of geographic location.

- When the **Entire Site** tab is selected, the grid displays rows of server groups.

- The single row of tabs that is initially displayed shows the NOAMP server groups followed by the SOAM server groups. The SOAM server groups indicate sites that are eligible for site upgrade.

- When a SG tab is selected, the grid displays rows of servers (as with ASG).

- If filtering has been applied, the **Entire Site** tab only displays when the result set for the site contains more than one server group.

> **Note:**
>
> The NO server group is not eligible for Automated Site Upgrade. When you select a SO server group from **Entire Site** on the **SO_SGx** tab., you can perform Site Upgrade on all servers in the SO's administrative domain.

Table 2-40   Upgrade Elements

Element	Description
Hostname	Lists the Hostname of the server.

Table 2-40   (Cont.) Upgrade Elements

Element	Description
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
	• 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 HA Role	The OAM HA role for this server. See HA Status Elements for more information.
Appl HA Role	The application HA role for the server.
Server Role	Role of this server in the system. Role is configured on the **Configuration**, and then **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**, and then **Server** page. For message processors, function is assigned on the related configuration page.
Upgrade Method (Entire Site)	The method to be used for this server group's upgrade. Methods are associated with SG functions by the application.
Server Upgrade States (Entire Site)	A list of the number of servers in each state in the server group, for example, Ready (1/2), Upgrading (1/2).
Server Application Versions (Entire Site)	A list of the number of servers in each state in the server group, for example, 7.2.0_72.41.8 (1/2), 7.2.0_72.41.9 (1/2).
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.

Table 2-40   (Cont.) Upgrade Elements

Element	Description
Entire site	• When the **Entire Site** tab is selected, some buttons are disabled because they only apply to selected server row(s), not selected SG row(s). These include **Backup** and **Checkup**. These are available when you are in an SG tab (using AW 6.0 ASG).
	• On the **Entire Site** tab, **Accept** is replaced with **Site Accept**. This allows you to accept all upgrades in the site by Server Group, much like **Backup All** and **Checkup All**.
	• When the **Entire Site** tab is selected, **Auto Upgrade** is changed to **Site Upgrade**. Clicking **Site Upgrade** generates a report of the planned upgrade order for all the servers in the site. You can then select an ISO and initiate the upgrade. If the site upgrade is already in progress, the form shows the status of each SG and each server.
	Note: If filtering has been applied, the Entire Site tab only displays when the result set for the site contains more than one server group.
Backup	Initiates backups on a server and server group basis based on the active server group tab.
Backup All	Initiates backups on a network element basis.
Checkup	Initiates upgrade health checks on a server and server group basis based on the active server group tab. This is enabled for all server group tabs. This is disabled on the active **Entire Site** tab.
Checkup All	Initiates upgrade health checks on a network element basis.
Upgrade Server	Enabled when one or more rows within the active server group tab are selected and the server is in the Ready state.
Upgrade Server or **Auto Upgrade** from the NO_SG tab	Initiates a server upgrade on servers with the action of upgrade. The form also allows the user to restart site upgrade on a partially upgraded site. **Note**: Upgrade is initiated according to the auto-upgrade policy on servers with an action of Auto Upgrade.
Site Upgrade or **Upgrade Server Group** from the Entire Site tab	Initiates a site upgrade. The form also allows the user to restart site upgrade on a partially upgraded site.

Table 2-40   (Cont.) Upgrade Elements

Element	Description
Site Upgrade	Moves to a form displaying the planned upgrade order for all the servers in the site. You can then select an ISO and initiate the upgrade. If the site upgrade is already in progress, the form shows the status of each SG and each server.
Site Accept	Initiates site accepts on a server group basis. This form is available only from the **Entire Site** tab, and it applies to servers in the current site only.
Auto Upgrade	Initiates the upgrade. Two upgrade modes are available; when no servers are selected, the button reflects **Auto Upgrade** and initiates a server group automated upgrade based on the active server group tab. When one or more servers are selected, the button toggles to **Upgrade Server** and initiates an upgrade only on the selected server(s).
Accept	Accept upgrade on the selected server(s) in the active server group tab.
Report	Generates a server report. Two report options are available; when no servers are selected, a report is generated for all servers in the server group. When one or more servers are selected, a report is generated only for the selected servers.
	When the **Entire Site** tab is displayed, the report contains information about the currently selected site. The report begins with the overall site upgrade status. If a site upgrade is in progress, the start time and running time are included. After this, the report includes the server groups in their upgrade sets (which shows the order of the site upgrade, whether in progress or planned). Each server group's upgrade method is also shown. The report also lists each server and its current status (Backup Needed, Ready, Upgrading, Failed, and so on) and its software version.
Report All	Generates a report for all servers in all server groups.
	When the **Entire Site** tab is displayed, this report shows all ongoing site upgrades in the topology (in case multiple sites are being upgraded simultaneously).

Overview of the Upgrade Procedure

The information in this section provides a general overview of the upgrade process. The user should always defer to the application specific upgrade instructions based on each release.

Follow these general steps when upgrading a server:

1. Backup your server.

2. Upload and verify the ISO image. (Refer to the sections on Uploading a Local File, Deploying an ISO file and Validating an ISO file.)

3. Initiate an upgrade.

4. Accept the upgrade.

> ⚠ **Caution:**
>
> Contact My Oracle Support and inform them of your upgrade plans before beginning this or any upgrade procedure. Before upgrading, go to the My Oracle Support website to acquire the correct upgrade procedure for your product and review any relevant Technical Service Bulletins (TSBs).

Overview of the Automated Site Upgrade Procedure

The information in this section provides a general overview of the automated site upgrade process. Always refer to the application specific upgrade instructions based on each release.

Follow these general steps when performing an automated site upgrade:

1. Upgrade the NO server group serially (one at a time) to ensure at least one NO is always active to provide OAM&P.

2. Upgrade the DRNO server group. Note that some products upgrade these first.

3. Select an SO network element and upgrade it as follows:

    • The SO servers can either be serial or bulk (non-active at once, then active) as specified in **General Options**.

    • Upgrade the MP servers using desired availability settings. The code uses the following rules (some of which can be specified by the user):

        – Servers are upgraded in parallel as long as the number of active, non-upgrading servers exceeds the user specified minimum availability.

        – Servers can be upgraded serially instead.

        – Servers are upgraded in HA order meaning Spare servers followed by Observer, Stby, and Active. An additional application-level customization allows certain servers to be upgraded last, once the rest of their group has upgraded.

4. Repeat step 3 until all SO network sites are upgraded (thereby completing upgrade of the entire network).

5. Accept the upgrade.

> ⚠️ **Caution:**
>
> Contact My Oracle Support and inform them of your upgrade plans before beginning this or any upgrade procedure. Before upgrading, go to the My Oracle Support website to acquire the correct upgrade procedure for your product and review any relevant Technical Service Bulletins (TSBs).

Backing Up Full Configuration Before an Upgrade

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

Two options are available to the user to perform a backup. The option **Backup** allows backups on a server and server group basis. The option **Backup All** allows backups on a network element basis.

Backing Up Using the Backup Option

Use the following procedure to initiate a server backup.

Servers must be in an appropriate upgrade state before initiating a backup. The appropriate upgrade states are **Backup Needed** or **Ready**.

> ✏️ **Note:**
>
> **Backup** is not available on the **Entire Site** tab.

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.
2. Select the appropriate server group tab that contains the target server(s).

   Target server(s) are displayed in the work area.
3. Optional: If you would like to selectively back up individual servers, highlight the server(s) from the listing.

   > ✏️ **Note:**
   >
   > If you would like to back up the entire server group, leave all servers unselected.

4. Click **Backup**.
5. On the Upgrade [Backup] form, click **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).
6. Click **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).

Upgrade Backup elements

Table 2-41 describes the elements on the Upgrade Backup form.

Table 2-41   Upgrade Backup Elements

Element	Description
Top Section	
Hostname	Hostname of the server.
Action	The action available during the backup. This field is not editable. Valid values include: • Back up • No back up
Current application version	The current version of the application.
Full Backup Options	
Database parts exclusion	Valid values are: • **Exclude** - performs a full backup of the COMCOL run environment, excluding the database parts specified in the files in the exclude_parts.d directory. • **Do Not Exclude** - performs a full backup of the COMCOL run environment without excluding any database parts, which is a longer procedure and produces larger backup files in the filemgmt directory.

Backing Up Using the Backup All Option

To create a full backup on a Network Element basis:

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Click **Backup All**.

3. On the Upgrade (Backup All) form all Networks Elements are selected for backup by default. Deselect any Network Elements that do not require a backup or alternatively, deselect **Action** and select any Network Elements required to be backed up. Take notice of the server list for all selected Network Elements. Confirm that all target servers are presented. If any target servers are not presented, click **Cancel** and review the server status.

4. In the **Full backup options** pane of the Upgrade (Backup All) form, click **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. Click **OK** to run the back up procedure.

The backup all process saves server information in the background for all servers of a selected network element group that are in the proper state for backup.

Upgrade Backup All elements

Table 2-42 describes the elements on the Upgrade Backup All form.

Table 2-42   Upgrade Backup All Elements

Element	Description
Top Section	
Network element	Name of the Network Element
Action	This action defines which Network Element is included in the backup. By default, all are selected. To limit the backup to a select group, deselect the Action checkbox and select which Network Elements are to be included in the backup.
Server(s) in the proper state for backup	Defines which servers in each Network element are in a proper state for backup.
Full Backup Options	
Database parts exclusion	Valid values are: • **Exclude** - performs a full backup of the COMCOL run environment, excluding the database parts specified in the files in the exclude_parts.d directory. • **Do Not Exclude** - performs a full backup of the COMCOL run environment without excluding any database parts, which is a longer procedure and produces larger backup files in the filemgmt directory.

Performing Upgrade Health Checks

Two buttons are located on the Upgrade administration page: **Checkup** and **Checkup All**. These let you perform upgrade health checks at various stages of the upgrade process. You can perform health checks on one or more selected server or servers, an entire server group, or more encompassing, on a network element basis. Additionally, the upgrade health check functionality is divided into four types: Advance Upgrade, Early Upgrade, Pre-Upgrade, and Post-Upgrade.

> **Note:**
>
> Depending on the application, any combination of the four types might be available presented. If only three types are available on the Upgrade [Checkup] or Upgrade [Checkup All] form, that means that the application supports those three types only.

See Upgrade Elements for more information about **Checkup** and **Checkup All**.

> **Note:**
>
> Some applications might not support health checks using **Checkup** and **Checkup All**. If your application does not to support this functionality, the buttons are on the Upgrade page, but they are disabled. You will not be able to navigate to the checkup forms.

> **⚠ Caution:**
>
> Depending on the application, the upgrade health check buttons might have different functionality than what is described in this content. Upgrade health checks should only be run as directed in the application upgrade guide for your specific release.

Upgrade health check using the checkup option

Use the following procedure to initiate an upgrade health check on an individual server or per server group basis.

> **Note:**
>
> The target ISO image file must be deployed before initiating a pre-upgrade health check. See Deploy an ISO File for more information. Additionally, a health check cannot be started on a server group or any individual servers in that group if another health check for that group is running. For example, a running network element based health check using the **Checkup All** option.

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.
2. Select the appropriate server group tab that contains the target server(s).
3. Optional: If you would like to selectively run a health check on individual server, highlight the server(s) from the listing.

> **Note:**
>
> To perform a health check on all servers in a server group, do not select any servers.

4. Click **Checkup**.
5. Select the appropriate **Checkup Type** using the options presented in the Health Check Settings pane.
6. Depending on the checkup type, you might be required to select the appropriate ISO image file from the Upgrade ISO list. Table 2-43 lists the options.

Table 2-43   Upgrade ISO Options

Option	Description
Advance Upgrade	The user may optionally choose the target ISO image file from the Upgrade ISO list.
Early Upgrade	The user may optionally choose the target ISO image file from the Upgrade ISO list.
Pre-Upgrade	The user is required to choose the target ISO image file from the Upgrade ISO list.
Post-Upgrade	No image selection is required. The ISO list is disabled.

7. Click **OK**.

The system initiates the health check. The user can monitor the progress of the task by selecting the **Tasks** list in the page control area. Once the task is complete, the user can access the results file either by selecting the active link under the details column in the **Tasks** list or by navigating to **Status & Manage**, and then **Tasks**, and then **Active Tasks**, selecting the appropriate server tab, and selecting the active link in the result details column. Either of these methods displays the Files page. See Files for information about managing files.

Upgrade health check checkup option elements

Table 2-44 describes the elements of the Upgrade [Checkup] form.

Table 2-44   Upgrade Checkup Elements

Element	Description
Top Section	
Hostname	Hostname of the server
Action	The action available during the upgrade health check. This field is not editable. Valid value is: • Health Check
Status	The current status of the server. Includes: • OAM Max HA Role • Appl Max HA Role (MP server groups only) • Network Element • Application Version
Health Check Settings	
Checkup Type	The upgrade health check type. Choices include: • Advance Upgrade • Early Upgrade • Pre-Upgrade • Post-Upgrade
Upgrade ISO	A list of available upgrade ISO media files. **Note**: This field is disabled for upgrade health checks of the type Post-Upgrade.
Submit Buttons	

Table 2-44   (Cont.) Upgrade Checkup Elements

Element	Description
OK	Submits the information to the server, and, if successful, returns to the View page for that table.
Cancel	Returns to the View page for the table without submitting any information to the server.

Upgrade health check using the checkup all option

Use the following procedure to initiate an upgrade health check on a network element basis.

> **Note:**
>
> The target ISO image file must be deployed before initiating a pre-upgrade health check. See Deploy an ISO File for more information. Additionally, a health check cannot be started if another health check is running. For example, a running health check on a server group or any individual servers using the **Checkup** option.

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Click **Checkup All**.

3. Select the target Network Elements using the checkboxes presented in the action pane. On the Upgrade [Checkup All] form, all Networks Elements are selected for check up by default. Deselect any Network Elements that do not require a check up or, alternatively, deselect Action and select any Network Elements requiring a health check. Note the server list for all selected Network Elements and confirm all target servers are presented. If any target servers are not presented, then select **Cancel** and review the server status.

4. Select the appropriate **Checkup Type** using the options presented in the Health Check Settings pane.

5. Depending on the checkup type, you might be required to select the appropriate ISO image file from the Upgrade ISO list. Table 2-45 lists the choices.

Table 2-45   ISO image file options

Option	Description
Advance Upgrade	(Optional) Select the target ISO image file from the Upgrade ISO list.
Early Upgrade	(Optional) Select the target ISO image file from the Upgrade ISO list.
Pre-Upgrade	Select the target ISO image file from the Upgrade ISO list.
Post-Upgrade	No image selection is required. The ISO list is disabled.

6. Click **OK**.

The system initiates the health check. The user can monitor the progress of the task by selecting the **Tasks** list in the page control area. Once the task is complete, the user can access the results file either by selecting the active link under the details column in the **Tasks** list or clicking **Status & Manage**, and then **Tasks**, and then **Active Tasks**, selecting the appropriate server tab, and selecting the active link in the result details column. Either of these methods displays the Files page. See Files for information about managing files.

Upgrade health check checkup all option elements

This table describes the elements of the Upgrade [Checkup All] form.

Table 2-46   Upgrade Checkup All Elements

Element	Description
Top Section	
Network element	Name of the Network Element.
Action	Defines which Network Elements are included in the checkup. By default, all are selected. To limit the checkup to a select group, deselect the Action checkbox and select which Network Elements are to be included in the checkup.
Server(s)	Defines the servers in each Network Element. This does not imply that each server is in the proper upgrade state to initiate a health check.
Health check options	
Checkup Type	The upgrade health check type. Option choices include: • Advance Upgrade • Early Upgrade • Pre-Upgrade • Post-Upgrade
Upgrade ISO	A list of available upgrade ISO media files. **Note**: This field is disabled for upgrade health checks of the type Post-Upgrade.
Submit Buttons	
OK	Submits the information to the server and, if successful, returns to the View page for that table.
Cancel	Returns to the View page for the table without submitting any information to the server.

Initiating Upgrades

You can choose to upgrade individual servers, server groups, or perform an automated upgrade for the entire site.

Chapter 2
Software Management

> **✎ Note:**
>
> Upgrade health checks, including health checks of the type **Early Upgrade** and **Pre-Upgrade**, should only be run as directed in the application upgrade guide for your specific release.

Individual Server Upgrade

Use the following procedure to initiate an individual server upgrade.

> **✎ Note:**
>
> The **Upgrade** menu choice is only available on the NOAM.

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Select one or more **Hostname(s**) on the **NO_SG** tab view..

3. Click **Upgrade Server**.

   The displayed GUI page shows configuration information about the selected Hostname.

4. Select the appropriate ISO media file from the **Upgrade ISO** list.

5. Click **OK**.

The system initiates the upgrade.

Initiate Server Upgrade elements

Table 2-47 describes the elements on the Initiate Upgrade form for individual server upgrades.

Table 2-47   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 list that contains the file names of available ISO images.

ORACLE®   2-59

Server Group Automated Upgrade

Use the following procedure to initiate an automated upgrade for an entire server group:

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Leave all servers unselected.

3. Click **Auto Upgrade**.

   The **Initiate Upgrade** form appears.

4. Select the appropriate **Mode** from the available listing.

   For information on the available upgrade settings, see Table 2-48.

5. For MPs only, select the desired **Availability** from the list.

   In serial upgrade mode **Availability** is not an option.

6. Select the appropriate ISO image from the **Upgrade ISO** list.

7. Click **OK**.

The system initiates the upgrade.

Initiate Server Group Upgrade elements

This table describes the elements on the Initiate Upgrade form for an automated Server Group upgrade.

> **Note:**
>
> For OAM server groups, HA groups are created according to the OAM HA Role of the server. The non-active HA role order is spare, observer and standby. For MP server groups, HA groups are created according to the Application HA Role of the server. The HA role order is spare, observer, standby and active.

The options in the Upgrade Settings section vary by server group type and are listed in Table 2-48.

Table 2-48   Initiate Upgrade Elements (Server Group)

Element	Description
Top Section	
Hostname	Hostname of the server.
Action	The action available during the upgrade. This field is not editable. Valid values include: • No upgrade • Upgrade • Auto Upgrade

Table 2-48   (Cont.) Initiate Upgrade Elements (Server Group)

Element	Description
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 list that contains the file names of available ISO images.
Mode	The server group upgrade mode. Valid values are: • Bulk - Upgrades all non-active OAM servers. For MPs only, upgrades servers according to availability setting in HA order • Serial - Upgrades individual servers sequentially in HA order • Grouped Bulk - Upgrades all non-active OAM servers by HA groups. For MPs only, upgrades servers in HA groups according to the availability setting
Availability	For MPs only. A list that specifies the desired percent availability of the servers in a server group during a bulk upgrade. Selecting **None** leads to all servers with an Action status of Auto Upgrade being unavailable.

Automated Site Upgrade

Use the following procedure to initiate an automated upgrade for an entire site.

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Select the SO SG tab corresponding to the site to be upgraded.

3. Select an **Entire Site**.

4. Click **Site Upgrade**.

5. Select an ISO.

6. Click **Site Accept** when ready to accept the upgrade. This action might need to take place based on site configuration or testing requirements, including time-sensitive requirements.

The system initiates the site upgrade.

Initiate Site Upgrade elements

Table 2-49 describes the elements on the Site Initiate Upgrade form for an automated Site upgrade.

Table 2-49   Site Initiate Upgrade Elements

Element	Description
Cycle	Displays the upgrade cycle in which the indicated servers will be upgraded.
Action	The configured upgrade type (depends on the selected ISO).
Server Group	Displays the server groups affected by the upgrade cycle.
Server	Displays the servers included in the upgrade (including Release).
Function	Displays the function of the server group. The function is provisioned by the application.

Accepting an Upgrade

After the server has successfully upgraded, run all health checks specified in the application upgrade guide. Accepting the upgrade confirms that the upgrade is correct and signals the end of the upgrade process.

> **Note:**
>
> Upgrade health checks, including health checks of the type **Post-Upgrade**, should only be run as directed in the application upgrade guide for your specific release.

> **Caution:**
>
> Once an upgrade is accepted, the backup configuration files are deleted and you cannot backout. It is not necessary to accept an upgrade immediately after completion. The decision may be made to test or soak the upgraded system before acceptance.

Use the following procedure to complete an upgrade:

1. Click **Administration**, and then **Software Management**, and then **Upgrade**.

2. Highlight the target server(s) from the listing.

3. Click **Accept** to complete the upgrade.

Generating an Upgrade Report

Use this procedure to generate a server report:

1. Click **Administration**, and then **Software management**, and then **Upgrade**.

2. Generate a report using one of the following options:

   • To generate a report for specific servers in a server group, click to select the server for which you want to create a report, and then click **Report**.

> **Note:**
>
> You can also use **Report** for a site upgrade report on the **Entire Site** tab.

- To generate a report for all servers in a server group, do not select any server in the group and click **Report**.
- To generate a report for all servers in all server groups, click **Report All**.

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

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 is 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

Table 2-50 describes the elements of the LDAP Authentication page.

Table 2-50   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-sensitive alphanumeric [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 account domain name (for example, 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 = 1-256 character alphanumeric
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]
		Default = (&(objectClass=user) (sAMAccountName=%s))
Account Canonical Form	Canonical Form for the provided username	Format: Options
		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. Click **Administration**, and then **Remote Servers**, and then **LDAP Authentication**.

2. Click **Insert** at the bottom of the table.

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, click **Test Server** 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. Click **Administration**, and then **Remote Servers**, and then **LDAP Authentication**.

2. Update LDAP settings as needed.

3. Click **OK** or **Apply** to submit the information.

The LDAP server changes are saved and activated.

ORACLE®

Generating a LDAP Authentication Report

Use this procedure to generate a LDAP Authentication report.

1. Click **Administration**, and then **Remote Servers**, and then **LDAP Authentication**.

2. Click **Report**.

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

The LDAP Authentication 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. Click **Administration**, and then **Remote Servers**, and then **LDAP Authentication**.

2. Select the appropriate host name from the listing for the LDAP Authentication server to delete.

3. Click **Delete**.

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

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

SNMP Trapping

The SNMP Trapping page enables the user to configure up to five remote managers to receive traps using the industry-standard Simple Network Management Protocol (SNMP). The user can choose between versions v2c, v3, or both along with the typical security parameters associated with each of the versions.

> **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.

A configuration mode option is provided that allows the user apply a configuration to all servers in the system or only to a specific site.

By default, system-wide traps are sent from the active Network OAM&P server while site-specific traps are sent from active Site OAM servers. Alternately, functionality may be enabled that allows individual servers to send traps, in which case individual servers interface directly with SNMP managers.

> **✎ Note:**
>
> Only the Active Network server allows SNMP administration. Global SNMP configuration cannot be modified if the disaster recover site is made Primary. It can be updated once original site becomes Primary again.

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. Table 2-51 describes the elements of the SNMP Administration page.

Table 2-51   SNMP Administration Elements

Element	Description	Data Input Notes
Configuration Mode	A configuration mode that determines whether the trap configuration is applied to all servers in the system or only to a specific site.	Format: Option Range: Global or Per-Site

Table 2-51   (Cont.) 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 IPv4, IPv6 address or a valid hostname. The port is optional, and can be specified by following the network address with a colon (:) and the port number. **Note**: IPv6 address must be encased in square brackets if the port is to be specified, for example, [address]:port. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001 Hostname Format: Alphanumeric [a-z, A-Z, 0-9] and minus sign (-) Hostname Range: 1 to 255-character string Port Format: Numeric Port Range: 1 to 65535 **Note**: If the port is not specified, the standard SNMP trap port of 162 is used. Default: No manager is configured.
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.

Table 2-51   (Cont.) SNMP Administration Elements

Element	Description	Data Input Notes
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: List Range: SNMPv2c, SNMPv3, or SNMPv2c and SNMPv3 Default: SNMPv2c and SNMPv3
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: Checkbox Range: Enabled or Disabled Default: Enabled
Traps from Individual Servers	Enables or disables SNMP traps from individualservers. If enabled, the traps are sent from individual servers, otherwise traps are sent from the Network OAM&P server.	Format: Checkbox 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.

ORACLE®

Table 2-51 (Cont.) SNMP Administration Elements

Element	Description	Data Input Notes
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: List Range: • 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: 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: List 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. Click **Administration**, and then **Remote Servers**, and then **SNMP Trapping**.

2. Select the desired **Server Group** tab.

3. Click **Insert**.

4. Update the options as appropriate.

   For more information regarding any field on this page, see SNMP Administration Elements.

5. Click **OK** 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:

1. Click **Administration**, and then **Remote Servers**, and then **SNMP Trapping**.
2. Select the desired **Server Group** tab.
3. Select the desired SNMP manager configuration by clicking on the line.
4. Click **Edit** to view the settings. When complete click **Cancel** if no changes are desired.

Updating SNMP Trap Settings

Use this procedure to update SNMP trap settings:

1. Click **Administration**, and then **Remote Servers**, and then **SNMP Trapping**.
2. Select the desired **Server Group** tab.
3. Select the desired SNMP manager configuration by clicking on the line.
4. Click **Edit** to view the settings
5. Update the options as appropriate.

   For more information regarding any field on this page, see SNMP Administration Elements.
6. Click **OK** to submit the information.

The SNMP trap changes are saved and activated.

Deleting SNMP Trap Managers or Configurations

Use this procedure to remove one or more SNMP trap managers or to delete the configuration in its entirety.

1. Click **Administration**, and then **Remote Servers**, and then **SNMP Trapping**.
2. Select the desired **Server Group** tab.
3. Select the desired SNMP manager configuration by clicking on the line.
4. To delete the entire configuration, click **Delete** and respond to the confirmation dialogue box.

   The entire **SNMP Trapping** configuration is deleted.
5. To delete a one or more managers, click **Edit**.
6. Identify the target manager and remove the IP address or hostname from the **Manager** field.

   For more information regarding this or any field on this page, see SNMP Administration Elements.
7. Click **OK** to apply the settings.

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.

Suspending and Resuming SNMP Trap Managers

Use this procedure to suspend or resume SNMP trap managers:

1. Click **Administration**, and then **Remote Servers**, and then **SNMP Trapping**.

2. Select the desired server group tab.

   The trap managers configured for that server group appear.

3. Select the desired trap manager. Click **Suspend** or **Resume** based on the current state. A dialogue box appears requesting confirmation. Confirm the choice.

The SNMP manager state changes.

Data Export

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

- Export Active Alarms
- Exporting Alarm and Event History
- Exporting KPIs
- #unique_145

For more information, see each individual section.

Data Export Overview

The Data Export page can be accessed from **Administration**, and then **Remote Servers**, and then **Data Export** under the main menu.

This feature allows you to create jobs to regularly transfer files or entire directories out of the file management area to a remote server using rsync.

- You can schedule up to 5 jobs to run per site (NO or SO)
- Each job can select one or more file management area subdirectories to include in the job.
- Each job can have its own schedule.
- Jobs can be tracked using the active tasks screen under status and manage. User defined tasks name can be applied for easy tracking. See Tasks for more information.

> **Note:**
>
> You are not limited to one remote server. Up to 5 different remote servers may be utilized.

Data Export pulls from files located in the file management area. Various automated and manual processes use the file management area to store files. These include the following types:

- Active Alarms (export task). See Export Active Alarms.

- Alarm and Event History (export task). See Exporting Alarm and Event History.

- Security Log (export task). See Exporting Security Log Files.

- KPIs (export task). See Exporting KPIs.

- Measurement Reports (export task). See Exporting Measurements Reports.

- Backups (depending on the application, this may include provisioning and configuration data).

Types designated as export tasks are scheduled by the user using forms accessed from the applicable page. It is important to understand that when you are scheduling an export task from one of these forms, you are not scheduling an export job to the remote server. You are scheduling an export task to the file management area. See Files for more information.

Files to be selected for export jobs are sourced from the file management area. Within the file management area, only files in the **export** and **backup** directories are eligible for export. Selecting the scope of files to be exported is accomplished by defining a directory path, starting with the **export** or **backup** directories, and using wildcards to include a desired range of files. A simple search using your favorite search engine explains wildcards and how to use them.

As the names infer, the **backup** directory hosts the backup files and the **export** directory hosts various performance indicators and log files generated by export tasks. See File Name Formats APDE for a description of directory structure and file name formats. For a practical view of files on your system, navigate from the GUI main menu to the **Status & Manage**, and then **Files** page and browse the various entries presented under each of the host tabs (this assumes some export tasks have already been executed).

Table 2-52 presents some examples when defining files to be transferred. Some of these examples may not be practical but convey a point.

Table 2-52   Data Export Examples

Files to Transfer	Description
export/*	Default value. Includes all subdirectories and files from the export directory.
backup/*	Includes all subdirectories and files from the backup directory.
export/*,/backup/*	Includes all subdirectories and files from both the backup and export directories.
export/<hostname>/*	Includes all export subdirectories and files from the specified host.
export/<hostname>/Events/*	Includes all events files from the specified host.
export/*/Events/*	Includes all events files from all hosts.

Table 2-52   (Cont.) Data Export Examples

Files to Transfer	Description
export/<hostname>/Events/*/*2016??01*	Includes all events files from the specified host and all network elements that occurred on the first day of each month in the year 2016 (The date segment is part of the file naming convention).
export/<hostname>/Alarms/*	Includes all alarm files from the specified host.
export/<hostname>/KPI/*	Includes all KPI files from the specified host.
export/<hostname>/Measurements/*	Includes all Measurements files from the specified host.
export/<hostname>/Seculog/*	Includes all Security Log files from the specified host.

When configuring an export job, the typical scheduling mechanisms are available. These include **Upload Frequency**, **Minute**, **Time of Day**, and **Day of Week**. The minimum export frequency is 15 minutes with the other options being hourly, daily, and weekly. Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. For example, if you were to select a frequency of daily, only the Time of Day list would be active. The minute list and the Day of Week buttons would be inactive and grayed out. See Data Export elements for information on the scheduling options.

File synchronization is managed using rsync. Depending on the OS and implementation of the remote server, it may be required to define the path to the rsync binary on the remote server. This is not common but an option is available to do that. Otherwise, this can be left blank. See Data Export elements for more information.

Several file compression choices are available, these include gzip, bzip2, and none. By default gzip is used. Based on scheduling, the compressed files are temporarily created on the local host once they are transferred to the remote server. The file compression choices can be made from the General Options form. See General Options Elements.

Data Export elements

Table 2-53 describes the elements on the **Administration**, and then **Remote Servers**, and then **Data Export**, and then **Insert/Edit** form.

Table 2-53   Data Export Elements

Element	Description	Data Input Notes
Task Name	Periodic export task name.	Format: Text box
		Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must be an alpha character or a number.
		Default: APDE Remote Server Copy
Task Description	Optional periodic export task description.	Format: Text box
		Range: Maximum length is 255 characters. Valid characters are alphanumeric, minus sign, underscore, and spaces between words. The first character must be an alpha character. The last character must be an alpha character or a number.
		Default: None
Remote Server	Name of export server.	Format: Text box
		Range: Maximum length is 255 characters. Valid hostname characters are alphanumeric, minus sign, and period. The Hostname must start with an alphanumeric and end with an alphanumeric. The top level domain (TLD) must be alphabetic.
		Note: Must be a valid hostname, IPv4 address, or IPv6 address.
		Default: None
Username	Username used to access the export server.	Format: Text box
		Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9).
		Default: None

Table 2-53   (Cont.) Data Export Elements

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: Text box
		Range: Maximum length is a 4096-character string. Valid characters are alphanumeric (a-z, A-Z, and 0-9), dash, underscore, period, and forward slash. If no directory is specified, the username's home directory on the remote server is used.
		Default: None
Path to rsync on Remote Server	Optional path to the rsync binary on the export server.	Format: Text box
		Range: Maximum length is a 4096-character string. Valid characters are alphanumeric (a-z, A-Z, and 0-9), dash, underscore, period, asterisk, and forward slash.
		Note: If no path is specified, the rsync-path option is not used.
Files to Transfer	Path to the files in the file management area on the local server to be transferred to the remote export server.	Format: Text combobox
		Range: Maximum length is a 4096-character string. Valid characters are alphanumeric (a-z, A-Z, and 0-9), dash, underscore, period, asterisk, and forward slash.
		Default: None
		Note: Combo box allows for several predefined options a user can select, or the user can type in a specific path. Path must be a subdirectory of backup/ or export/. If no directory is provided, the default directory is set to export/*.
Upload Frequency	Frequency at which the export occurs.	Format: Options
		Range: fifteen minutes, hourly, daily, or weekly
		Default: weekly
		Note: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out.

Table 2-53   (Cont.) Data Export Elements

Element	Description	Data Input Notes
Minute	Select the minute of each hour when transfer begins. Enabled only if Upload Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list Range: 0 to 59 Default: 0 **Note**: The Minute selection is only active if the selected Upload Frequency is either Fifteen Minutes or Hourly.
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time text box Range: HH:MM with AM/PM Default: 12:00 AM **Note**: The Time of Day selection is only active if the selected Upload Frequency is either Daily or Weekly. Select from 15-minute increments or fill in a specific value.
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly..	Format: Options Range: Sunday through Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Configure Data Export Jobs

The Data Export [Insert] form enables you to configure a single data export job to send files to a remote server. You are allowed to configure up to five jobs per site.

1. From the main menu, click **Administration**, and then **Remote Servers**, and then **Data Export**.

   The Data Export page is presented with a grid displaying any currently configured export servers.

2. Click **Insert**.

3. Enter a **Task Name**.

4. Enter a **Task Description**.

5. Enter a **Remote Server** Name, IPv4, or IPv6 address.

   See Data Export elements for details about the **Remote Server** field and other fields that display on this page.

6. Enter a **Username**.

7. Optional: Enter the **Directory on Export Server**.

   This is the target directory path on the export server.

8. Optional: Enter the **Path to Rsync** on the remote server.

> **Note:**
>
> Depending on the OS and implementation of the remote server, it may be required to define the path to the rsync binary on the export server but this is not common. If no path is specified, the username's home directory on the export server is used.

9. Select or enter the **Files to Transfer** path(s).

   This entry defines the path(s) to the files within the File Management Area from which files are exported. A combobox allows for one of several predefined options to be selected, or the user can type in a specific path. Multiple paths may be entered.

10. Select the **Upload Frequency**.

11. If you selected fifteen minutes or hourly for the upload frequency, select the **Minute** for which the transfer is set to begin.

> **Note:**
>
> This is the minute of each period when the transfer is set to begin. For an Upload Frequency of Fifteen Minutes, transfers occur four times per hour, and this field sets the minute of the first transfer in the hour.

12. If you selected daily or weekly for the upload frequency, select the **Time of Day**.

13. If you selected weekly for the upload frequency, select the **Day of the Week**.

14. Click **OK** to apply the changes or **Cancel** to discard the changes.

    The export job configuration is saved and you are returned to the Data Export page. A grid is presented reflecting the newly added job.

15. If public keys were manually placed on the remote server, skip to step 17; otherwise, select the newly added export job by clicking on it and click **Key Exchange**. This button initiates a key exchange between the local OAM server and the data export remote server currently defined in the job. See Generate a Data Export Keys Report.

16. Enter the password.

    A password must be entered before the exchange can complete. The server attempts to exchange keys with the remote server. After the keys are successfully exchanged, continue with the next step.

17. Optional: Select the newly updated export job by clicking on it. Click **Test Transfer** to confirm the ability to export to the remote server.

    The user can monitor the progress of the task by selecting the **Tasks** list in the page control area.

The export job is now configured and active.

Update Data Export Jobs

The Data Export [Edit] form enables you to modify the existing configuration settings of a specific export job.

1. From the main menu, click **Administration**, and then **Remote Servers**, and then **Data Export**.

   The Data Export page displays with a grid displaying currently configured export jobs.

2. Select the desired export job by left clicking on it and click **Edit**.

3. Make the desired changes. Note that some options are not available to change and the buttons, text boxes, or lists are grayed out. Some options may become active based on other selections, for example, **Upload Frequency**.

4. Click **OK** to apply the changes or **Cancel** to discard the changes.

   If **OK** was selected, the export job configuration is saved and you are returned to the Data Export page.

5. Optional: Select the newly updated export job by clicking on it. Click **Test Transfer** to confirm the ability to export to the remote server.

   The user can monitor the progress of the task by selecting the **Tasks** list in the page control area.

The export job is now updated and active.

Delete Data Export Jobs

The Data Export page has a button that enables you to delete one or more data export jobs.

1. From the main menu, click **Administration**, and then **Remote Servers**, and then **Data Export**.

   The Data Export page is presented with a grid displaying currently configured export jobs.

2. From the grid, click to select the export job you want to delete. Alternately, you can delete multiple export jobs. To delete multiple jobs, press and hold **Ctrl** and click to select multiple jobs.

3. Click **Delete** and respond to the confirmation dialogue box that is presented.

4. Click **OK** to delete the export job(s).

Data Export Transfer Now

The Data Export page has a button that enables you to initiate an immediate attempt to transfer any data files in the user defined directory to the remote server without having to wait for a scheduled period to arrive. Only a single export job may be selected for each attempt.

1. From the main menu, click **Administration**, and then **Remote Servers**, and then **Data Export**.

   The Data Export page displays with a grid displaying the currently configured export jobs.

2. From the grid, click to select the desired export job. Click **Tranfer Now** to initiate an immediate attempt to transfer the data files and respond to the confirmation screen that displays.

3. Click **OK** to initiate the transfer.

The file transfer is initiated. The user can monitor the task or simply check the export directory on the remote server for success.

Generate a Data Export Keys Report

The **Keys Report** button located on the Data Export page generates a report that contains the root public key of the local OAM server in the associated network element. The key can then be added to the remote server to allow RSYNC transfer of exported data files from the selected OAM server.

> **Note:**
>
> The **Keys Report** function is available regardless of whether a data export job is currently defined or not.

The report can be printed, or saved to a file.

Use this procedure to generate a data export keys report.

1. Click **Administration**, and then **Remote Servers**, and then **Data Export**.

2. Click **Keys Report**.

   The Data Export [Report] page displays the public key of the local OAM server.

3. Click **Print** to print the report, or click **Save** to save the file locally to your client workstation. Click **Back** to return you to the Data Export page.

The keys report contains detailed instructions on how to add these public keys to the remote server.

DNS Configuration

The DNS Configuration page can be accessed by navigating from the main menu to **Administration**, and then **Remote Servers**, and then **DNS Configuration**.

The page presents a single row of tabs. Each tab represents a network element and all servers participating in that network element. In addition to the tabs, the page also presents **Insert**, **Edit**, and **Delete** buttons. These buttons are active or inactive based on the presence of (or lack of) an active DNS configuration.

> **Note:**
>
> Only one DNS server is allowed to be configured per network element.

Once a DNS configuration has been applied, the page displays the name server and address as well as each of the defined search domains for that name server.

A DNS configuration can be applied globally to the system or to a specific network element. The DNS configuration is considered in **GLOBAL** mode if only a NO configuration exists. Otherwise, it's per-site. Put another way, if a single DNS configuration is only applied to the NO network element and no other tab receives a configuration then the DNS configuration is in **GLOBAL** mode and serves all the network elements. If two or more DNS configurations are applied to the system the

configuration is in **SITE** mode. If no DNS configuration is applied then the system is in **UNCONFIGURED** mode. To determine the current mode of the system access the **Info** list.

> **Note:**
>
> Once the system is in **SITE** mode, any network element tab not containing a DNS configuration is excluded from accessing a DNS server. If you want all network elements to have access to a DNS name server while the system is in **SITE** mode then each tab must be configured even if they use the same name server and search domains.

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

- DNS Configuration Elements
- Adding a DNS Configuration
- Updating a DNS Configuration
- Deleting a DNS Configuration

DNS Configuration Elements

The DNS Configuration [Insert] form provides for configuration of the domain name system. Table 2-54 describes the elements of the DNS Configuration [Insert] form.

Table 2-54   DNS Configuration Elements

Element	Description	Data Input Notes
External DNS Name Server		
Name Server	Address of external DNS name server. [Must be a valid ipv4 or ipv6 address]	Format: Valid IPv4 or IPv6 address Range: (IPv4) or colon hex (IPv6)
Domain Search Order		
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

Table 2-54   (Cont.) DNS Configuration Elements

Element	Description	Data Input Notes
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
Submit Buttons		
OK	Submits the information to the server, and, if successful, returns to the DNS Configuration page.	
Cancel	Returns to the DNS Configuration page without submitting any information to the server.	

Adding a DNS Configuration

Use this procedure to add a DNS Configuration:

1. Click **Administration**, and then **Remote Servers**, and then **DNS Configuration**.

2. Select the tab representing the desired network element.

3. Click **Insert**.

4. Enter a **Name Server** using a valid IPv4 or IPv6 address.

5. Enter the **Search Domain** in the domain search order. You may add up to six search domain names.

6. Click **OK** 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. Click **Administration**, and then **Remote Servers**, and then **DNS Configuration**.

2. Select the tab representing the desired network element.

3. Click **Edit**.

4. Update the information on the DNS **Configuration [Insert]** form and click **OK** to submit the new information.

The updated DNS configuration is saved and activated.

Deleting a DNS Configuration

Use this procedure to delete a DNS configuration:

> **Note:**
>
> Before deleting a configuration, note the DNS configuration mode. Deleting a DNS configuration from the NO network element while the system is in **GLOBAL** mode affects all network elements relying on DNS service.

1. Click **Administration**, and then **Remote Servers**, and then **DNS Configuration**.
2. Select the tab representing the desired network element.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.
5. Confirm the DNS configuration has been deleted by navigating to the desired network element tab and confirming that the **No DNS configured** message is displayed.

The DNS configuration has been deleted.

3

Configuration

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 used by middleware to control data replication and data collection, and define HA relationships.

Networking

Found under the main menu sub-directory of **Configuration**, and then **Networking** is a collection of pages which allow the user to configure networks, devices, and routes. Additionally, application services are mapped to networks via the Services page.

Networks

The Networks page is used to create the networks used for internal, external, and signaling communications. The networks are grouped into logical buckets called network elements. Only after creating these buckets can the networks themselves be defined. One advantage of this architecture is simplified network device configuration and service mapping.

The workflow is to first create the network elements and then define the individual networks inside each element.

Network Elements

A network element is simply a collection of networks. In other words, a container of networks. Any servers belonging to a specific network element uses those networks exclusively to communicate internally and externally. A network element can contain multiple servers but a single server can only belong to one network element.

Using a three-tier DSR system as an example, a typical, regionally diverse, signaling network would have multiple network elements. Consider a system deployed across an east region and west region. The network element configuration might look like:

- NO_East
- NO_West
- SO_East
- SO_West
- NO_DR (Disaster Recovery Spare)

> ⚠️ **Caution:**
>
> Depending on the application, the workflow and provisioning instruction may differ from the direction provided here. Always follow the provisioning guidelines for your specific application and release.

There are two methods for creating network elements. The first method involves manual entry using the Networks [Insert network Element] form. See Inserting a network element for more information on this method. The second method is more encompassing and allows the user to simultaneously create the network element and associated networks. See Uploading a network element configuration file.

Networks Insert Network Element

Table 3-1 describes the elements of theNetworks [Insert Network Element] form.

Table 3-1   Insert Network Elements Elements

Field	Description	Data Input Notes
Network Element Name	The user-defined name for the network element.	Must be unique.
		Format: String
		Range: 1-32 alphanumeric characters and underscore. Must contain at least one alphabetic character and must not start with a digit.
		Default: n/a
		A Value is required.

Inserting a network element

This procedure defines the manual process of inserting a network element. To view the procedure that involves the uploading of a network element configuration file see Uploading a network element configuration file.

Use this procedure to define and insert a network element:

1. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Click **Insert Network Element**.

3. Enter a unique name in the value field for **Network Element Name**.

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

   See Network Insert elements for value limitations of the **Network Element Name** field.

5. Click **OK** to submit the information and return to the Networks page or **Cancel** to discard the changes and return to the Networks page.

The network element is added to the topology database tables, and the GUI displays the newly added network element in tab format on the Networks page.

Uploading a network element configuration file

This procedure defines the automated process of uploading a network element configuration file to create the network element. To view the procedure that involves the manual process of inserting a network element see Inserting a network element.

> **Note:**
>
> Depending on the application, the workflow and provisioning instruction may differ from the direction provided here. Because applications differ, the format of the configuration file is not addressed here. Always follow the provisioning guidelines for your specific application and release.

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

1. Click **Configuration**, and then **Networking**, and then **Networks**.

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

   A file upload screen displays allowing you to navigate to and select the target configuration file.

3. Select the target file and click **Open**.

   The screen disappears and the target file displays in the text box to the right of the **Browse** button.

4. Click **Upload File**.

   The file is uploaded and data validation is performed.

Data validation is performed immediately. If the file is valid, a new network element is created and reflected in a new tab on the Networks page. 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. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located in the tool bar area to the right or left of the visible tabs.

Deleting a Network Element

Before deleting a network element the user must ensure that no servers are associated with the target network element. Attempting to delete a network element with at least one associated server results in an error message and the target network element is not deleted. If a network element contains networks, but is not associated with any servers, then deleting the network element is successful. The networks contained in the target network element are deleted along with the network element.

Use this procedure to delete a network element after confirming that no servers are associated with it:

1. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate the target network element tab.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click the **x** located on the tab of the target network element.

   A delete confirmation message appears.

4. Click **OK** to delete the network element from the database tables.

   A status message is presented stating the network element has successfully been deleted. Closing the status message returns you to the Networks page.

The network element and related networks are deleted from the databases.

Exporting a network element configuration file

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

1. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Select the target network element tab.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click **Export**.

   A file dialogue box appears prompting you to open or save the configuration file. By default the name format of the output file is NE_<yyyymmdd>_<hhmmss>_<zone>.xml. You may change this as needed.

Network Insert elements

Table 3-2 describes the elements of the Networks Insert form.

Table 3-2   Networks Insert Elements

Field	Description	Data Input Notes
Network Name	The name of the network.	Must be unique.
		Format: String
		Range: 1-31 alphanumeric characters. Must start with a letter. No special characters are allowed.
		Defaut: n/a
		A value is required.

Table 3-2   (Cont.) Networks Insert Elements

Field	Description	Data Input Notes
Network Type	The type of network in the context of the application.	Format: List Range: OAM or Signaling Default: OAM
VLAN ID	The VLAN ID of the Network	Format: Numeric Range: 1-4094 A value is required.
Network Address	The network address of the Network	Format: Valid network address Range: Dotted decimal (IPv4) or colon hex (IPv6) Default: n/a A value is required.
Netmask	Subnetting to apply to servers within the Network	Format: Valid network netmask Range: Prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4) Default: n/a A value is required.
Router IP	The IP address of a router on this network. **Note**: If this is a default network, this i used as the gateway address of the default route on servers with interfaces on this network. If customer router monitoring is enabled, this address is the one monitored.	Format: Valid IP address Range: Dotted decimal (IPv4) or colon hex (IPv6) Default: n/a **Note**: A value is not required. Networks without a router IP cannot be used as the default network. The default network selection defaults to No.
Default Network	Whether the network is the default gateway	Format: Option Range: Yes or No
Routed	Whether the network is routed outside its network element. **Note**: The network is automatically assigned to a network element when a server in a network element has an IP from the network assigned is to it. If it is not assigned to a network element, it is assumed to be possibly present in all network elements.	Format: Option Range: Yes or No **Note**: Select No to allow the same IMI network/IPs to be used at multiple Signaling sites.

Inserting a Network

Use the following procedure for manually inserting a network. Alternatively, you can use the automated process of uploading a network element configuration file to create both the network element and associated networks. See Uploading a network element configuration file.

1. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate and select the target network element tab where you want to create the network.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click **Insert**.

4. Enter a **Network Name**.

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

5. Select a **Network Type** from the list.

6. Enter a **VLAN ID**.

7. Enter a **Network Address**.

   This is a network address and not a host IP address.

8. Enter a **Netmask**.

9. Optional: Enter the **Router IP**

   This is used as the gateway address of the default route if yes is chosen in step 10.

10. Choose whether this will be the network with a default gateway.

    If yes is chosen, the gateway address entered in step 9 acts as the default route for servers with interfaces on this network.

11. Choose whether this network is routed outside its network element.

12. Click **OK** to submit the information and return to the Networks page, or click **Apply** to submit the information and continue entering additional data. Clicking cancel discards your changes and returns you to the Networks page.

The new network is added to the target network element.

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 a route or a device to a network, the network would have to be in an unlocked state.

1. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate and select the network element tab where the network you want to unlock exists.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Identify the target network and determine the lock status. This can be accomplished by identifying the value of the **Locked** field for your target network. A value of yes indicates the network is currently locked; no indicates the network is not currently locked. Alternatively, you can select the target network and take note of the **Lock/Unlock** button. If the button transitions to **Unlock** then the network is currently locked; if the button transitions to **Lock** then the network is currently unlocked.

4. To unlock a locked network, click **Unlock** and respond to the confirmation screen displayed. When unlocking you also have to confirm your decision using a checkbox.

   The network is now unlocked.

5. To lock an unlocked network, click **Lock** and respond to the confirmation dialogue box that is presented.

   The network is now locked.

The network is locked or unlocked.

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:**
>
> Before editing a network, generate a network report. The network report serves 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. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate and select the network element tab where the network you want to edit exists.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Select the target network and determine the lock status. If the network is currently unlocked proceed to the next step. If the network is locked the **Lock/Unlock** button should be active and reflect **Unlock**. Click **Unlock** and respond to the confirmation dialogue box that is presented.

   The network is now unlocked.

4. Navigate back to the target network elements tab and select the target network again. Click **Edit**.

   If the network cannot be edited it means it is still locked or it is a pre-configured network.

5. Edit the available fields as necessary.

   See Network Insert elements for details about the fields that display on this page.

> ✎ **Note:**
>
> Fields that cannot be edited are disabled.

6. Click **OK** to submit the changes and return to the Networks page, or click **Apply** to submit the information and continue editing additional data. Clicking cancel discards your changes and returns you to the Networks page.

7. Return the target network to the desired lock status.

The network is changed.

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:**
>
> Before deleting a network, generate a network report. The network report serves 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. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate and select the network element tab where the network you want to delete exists.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click to select the network you want to delete. To delete multiple networks, press and hold **Ctrl** and click to select multiple networks.

   If the network cannot be deleted, **Delete** is disabled. To delete multiple networks at one time, all selected networks must be deletable.

4. Click **Delete** and respond to the confirmation dialogue box that is presented.

5. Click **OK** to delete the network.

The network has been removed from the database and it no longer displays in the network element tab.

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. Click **Configuration**, and then **Networking**, and then **Networks**.

2. Locate and select the network element tab where the target networks exist.

   Network elements are presented in tabular form. If the target network element is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. 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**. To generate a report for multiple networks, press and hold **Ctrl** as you click to select specific networks.

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

Devices

The Devices page is used to configure and manage additional interfaces other than what was configured during the initial installation.

Devices Elements

Table 3-3 describes the elements of the Devices page.

Table 3-3   Devices Elements

Tab/Field	Description
Server	The server host name displayed in tabbed format at the top of the table
Device Name	The name of the device (not user defined)
Device Type	The device type. Supported types include: • Bonding • Vlan • Alias • Ethernet
Device Options	A collection of keyword value pairs for the device options
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 pending) • Deployed (provisioned through the GUI; server update is complete) • Pending (edit or delete update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)
Is Locked?	Status of the lock state. The possible states are: • Locked (Not available for edit or delete) • Unlocked (Available for edit or delete)

Viewing a Device

Devices are viewed on per server basis. The use of italics indicates a device that cannot be edited or deleted.

Use this procedure to view devices:

1. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab.

   Servers are presented in tabbed form. If the target server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

The devices for that selected server are displayed.

Device Insert Elements

Table 3-4 describes the elements of the Devices [Insert] form.

> **Note:**
>
> Some fields are dynamic and only display when specific values are selected. Dynamic fields are noted in the description.

Table 3-4   Devices General Options

Field	Description	Data Input Notes
Device Type	The type of device. **Note**: A device type of **Ethernet** is system generated and not selectable from this form.	Format: Options Range: Bonding, VLAN, Alias Default: N/A A value is required.
Start on Boot	When selected, this checkbox enables the device to start on boot.	Format: Checkbox Default: Enabled
Boot Protocol	The boot protocol.	Format: List Range: None, DHCP Default: None A value is required.
MTU Setting	The Maximum Transmission Unit (MTU) setting for the device (bytes per packet) **Caution**: Changing the MTU setting for an existing interface restarts the interface, which is service affecting.	Format: Numeric Range: 1280-65570 Default: 1500
Monitoring Type	The monitoring type to use with a bonding device. **Note**: This field is dynamic and only displays when bonding is selected as the device type.	Format: Options Range: MII, ARP Default: MI A Value is required.
Primary	The preferred primary interface. **Note**: This field is dynamic and only appears when bonding is selected as the device type and a monitoring type choice is selected.	Format: List Range: None - all available devices Default: None A value is required.

Table 3-4   (Cont.) Devices General Options

Field	Description	Data Input Notes
Monitoring Interval	MII monitoring interval in milliseconds. **Note**: A monitoring type is selected by default (MII).	Format: Numeric Range: A positive integer Default: 100ms A value is required.
Upstream Delay	MII monitoring upstream delay in milliseconds. **Note**: This field is dynamic and only appears when bonding is selected as the device type and MII is selected as the monitoring type.	Format: Numeric Range: A positive integer Default: 200ms A value is required.
Downstream Delay	MII monitoring downstream delay in milliseconds. **Note**: This field is dynamic and only appears when bonding is selected as the device type and MII is selected as the monitoring type.	Format: Numeric Range: A positive integer Default: 200ms A value is required.
ARP Validation	The method to validate the ARP probes and replies. **Note**: This field is dynamic and only appears when bonding is selected as the device type and ARP is selected as the monitoring type.	Format: List Range: None, Active, Backup, All Default: None A value is required.
ARP Target IP(s)	Comma-separated ARP target IP address list. **Note**: This field is dynamic and only appears when bonding is selected as the device type and ARP is selected as the monitoring type.	Format: Valid IP addresses Range: Dotted quad decimal (IPv4) or colon hex (IPv6) Default: None Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
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. This cannot be changed after the device is created.	Format: Options Range: Available base devices Default: N/A A Value is required.
IP Interfaces		
Add IP Interface	Presents a row with a single address box and network list. **Note**: For each row, only one IP Address and network can be specified. To specify additional rows, click**Add IP Interface**.	Format: Button At least one entry is required.

Table 3-4   (Cont.) Devices General Options

Field	Description	Data Input Notes
Remove	Removes the device interface IP Address on the selected row. **Note**: This is not a delete button. If**Apply** has already been selected, clicking**Remove** does not delete the interface. Deleting an interface that has already been defined takes place from the Devices page.	Format: Button
Submit Buttons		
OK	Submits the information to the database, and, if successful, returns you to the Devices page.	
Apply	Submits the information to the database, and, if successful, remains on the Devices [Insert] form so that you can enter additional data.	
Cancel	Discards the information and returns you to the Devices page.	

Inserting a Device

The Devices [Insert] form uses dynamic options. Depending on the selected value of a field, options may be added or removed from the form. It is important to review and understand the elements associated with this form by reviewing the Device Insert Elements page.

> **Note:**
>
> Devices cannot be created that 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. Additionally, device creation requires that the prerequisite networks are already configured. See Inserting a Network for more details.

1. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab.

   Servers are presented in tabbed form. If the target server is not visible in the available screen space, use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click **Insert**.

4. Select the **Device Type**. If the selected device type is **Bonding**, then continue with this step; otherwise, skip to 5.

   a. By default, **Start on Boot** is enabled. Uncheck the checkbox if you want to disable **Start on Boot**.

   b. Select the **Boot Protocol**.

   c. Enter the **MTU Setting** if a default of 1500 is not desired.

   d. Select the **Monitoring Type**.

   e. Select the **Primary** interface.

   f. Enter the **Monitoring Interval**.

   g. If MII was selected as the monitoring type, then enter the **Upstream Delay** in milliseconds; otherwise, skip to substep 4.j.

   h. Enter the **Downstream Delay** in milliseconds.

   i. Select **Base Devices**. Two must be selected.

   j. If ARP was selected as the monitoring type, then enter the **ARP Validation** method.

   k. Enter the **ARP Target IP(s)** using valid comma separated IP addresses.

   l. Skip to step 7 to continue.

5. If the selected device type is **VLAN**, then continue with this step; otherwise, skip to 6.

   a. By default, **Start on Boot** is enabled. Uncheck the checkbox if you want to disable **Start on Boot**.

   b. Select the **Boot Protocol**.

   c. Enter the **MTU Setting** if a default of 1500 is not desired.

   d. Select **Base Device**. Only one can be selected.

   e. Skip to step 7 to continue.

6. If the selected device type is **Alias**, then continue with this step; otherwise, skip to 7.

   a. By default, **Start on Boot** is enabled. Uncheck the checkbox if you want to disable **Start on Boot**.

   b. Select the **Boot Protocol**.

   c. Enter the **MTU Setting** if a default of 1500 is not desired. This is not an option for Alias device.

   d. Select **Base Device**. Only one can be selected.

7. Click **Add IP Interface**.

   A new row is created with a textbox and list.

8. Enter an **IP Address** for the device.

9. Select a **Network Name** from the list.

10. For each row, only one IP Address and Network Name can be specified. To specify additional interfaces, select **Add IP Interface** and complete steps 8 and 9.

11. When you are finished adding IP addresses, click **OK** to submit the information and return to the Devices page, or click **Apply** to submit the information and

continue entering additional data. Clicking **Cancel** discards your changes and returns you to the Devices page.

Taking Ownership of a Device

Devices that have a configuration status of **Discovered** are devices that were configured during the initial install or extension process and not added manually. The user has limited abilities to modify these devices. When you need to edit the attributes of these devices, you must first take ownership of the device.

Before taking ownership of a device, the user should be familiar with the concept of locked/unlocked networks. Before editing or deleting any device that belongs to a locked network, the network must be unlocked. See Locking and Unlocking a Network for more information.

> **Note:**
>
> Not all devices must belong to a network. For example, primary interfaces with a state of **Discovered** may not belong to a network.

The process of taking ownership of a device and then editing or deleting that device slightly differs depending on whether or not that device currently belongs to a locked network. See Editing a Device for more information.

Before taking ownership of a discovered device, the device has a configuration status of **Discovered; Locked**. **Edit** and **Delete** are disabled. Immediately after taking ownership of the device, the configuration status temporarily changes to **Configured** and then **Pending**. Within a few minutes, the device should transition to its final configuration status of **Deployed**. If the device belonged to a locked network before taking ownership, the status displays as **Deployed; Locked**, otherwise it displays as **Deployed; Unlocked**.

> **Note:**
>
> Before taking ownership of a device, generate a device report. The device report serves 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.

Use the following procedure to take ownership of a device.

1. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab where the target device exists.

   Servers are presented in tabbed form. If the target server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

   The device data for the selected server appears.

3. Click to select the device you want to take ownership of. Alternately, you can take ownership of multiple devices. Press and hold **Ctrl** and click to select more than one device.

If one or more selected devices have a configuration status of something other than **Discovered**, the **Take Ownership** button is disabled. To take ownership of multiple devices at one time, all selected devices must have a configuration status of **Discovered**.

4. Click **Take Ownership**.

The configuration status temporarily displays **Configured**, then **Pending**, and finally **Deployed**.

The devices are now available for editing or deleting. Take note of the lock status. A device cannot be edited or deleted while in the **Locked** state. See Locking and Unlocking a Network for details on changing the lock status.

Editing a Device

Devices with a locked status cannot be edited without unlocking the network to which they belong. See Locking and Unlocking a Network for more information. Additionally, devices that have a configuration status of discovered cannot be unlocked until you take ownership of the device. See Taking Ownership of a Device for more information. Some discovered devices not belonging to a network are unlocked immediately after taking ownership. Other discovered devices require the extra step of unlocking the network after taking ownership.

> ✎ **Note:**
>
> Before editing a device, generate a device report. The device report serves 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. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab.

Servers are presented in tabbed form. If the target server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

The device data for the selected server appears.

3. Click to select a device and click **Edit**.

If the device cannot be edited, **Edit** is disabled. Confirm the device is in a deployed and unlocked state. If the device can be edited, the Devices [Edit] form 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.

> **⚠ Caution:**
>
> Changing the MTU setting for an existing interface restarts the interface, which affects service.

5. Click **OK** to submit the information and return to the Devices page, or click **Apply** to submit the information and continue entering additional data. Clicking cancel discards your changes and returns you to the Devices page.

The device is changed.

Deleting a Device

Devices with a locked status cannot be deleted without unlocking the network to which they belong. See Locking and Unlocking a Network for more information. Additionally, devices that have a configuration status of discovered cannot be unlocked until you take ownership of the device. See Taking Ownership of a Device for more information. Some discovered devices not belonging to a network are unlocked immediately after taking ownership. Other discovered devices require the extra step of unlocking the network after taking ownership.

> **✎ Note:**
>
> Before deleting a device, generate a device report. The device report serves 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. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab.

    Servers are presented in tabbed form. If the target server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

    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.

    If the device cannot be deleted, **Delete** is disabled. Confirm the device is in a deployed and unlocked state. To delete multiple devices at one time, all selected devices must be deletable.

4. Click **Delete**.

5. Click **OK**.

Generating a Device Report

A device report can be generated on a single device, multiple devices within the same server, or all devices regardless of server.

1. Click **Configuration**, and then **Networking**, and then **Devices**.

2. Locate and select the desired server tab.

Servers are presented in tabbed form. If the target server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

The device data for the selected server displays.

3. To generate a device report, select one of the following procedures:

• To generate a report for all devices under the current server tab, click **Report**.

• To generate a report for a single device, click to select the device and click **Report**. Alternatively, you can select multiple devices. To generate a report for multiple devices, press and hold **Ctrl** as you click to select specific devices.

• To generate a report for all devices regardless of server, click **Report All**.

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 traffic. You can specify routes for the entire network, specific servers, or specific server groups.

Routes Elements

Table 3-5 describes the elements of the Routes page.

Table 3-5   Routes Elements

Tab/Field	Description
Server Group/Server	Server groups are presented in tabs at the top of the main work area. Selecting a specific server group reveals the individual servers of that group. Alternatively, selecting the **Entire Network** tab reveals all the servers defined in the system. After selecting a specific server group, the user has the option of selecting a specific server or selecting **Entire Server Group** to reveal the existing routes.
Route Type	The type of route. Possible types are: • Net (A route that serves a specific network) • default (The default route for that server) • Host (A route to a specific target host)
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
Device Name	The network device through which traffic is being routed. **Note**: This is not available on the **Entire Server Group** tab.

Table 3-5   (Cont.) Routes Elements

Tab/Field	Description
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 scoped routes.
Route Scope	The scope of the route. Possible types are server and server group.
	Note: This column is only present for server sub-tabs.
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 pending)
	• Deployed (provisioned through the GUI; server update is complete)
	• Pending (edit or delete update in progress)
	• Deferred (server cannot be reached for updates)
	• Error (specific error text is displayed in the Configuration Status field)
Is Locked?	Status of the lock state. The possible states are:
	• Locked (Not available for edit or delete)
	• Unlocked (Available for edit or delete)

Viewing a Route

Use this procedure to view current routes.

1. Click **Configuration**, and then **Networking**, and then **Routes**.

2. Click to select a server group and/or server using the tabs at the top of the main work area.

   If the target server group or server is not visible in the available screen space use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs. Server groups are presented in tabs at the top of the main work area. Selecting a specific server group reveals the individual servers of that group. Alternatively, selecting the **Entire Network** tab reveals all the servers defined in the system. After selecting a specific server group, the user has the option of selecting a specific server or selecting **Entire Server Group** to reveal the server group scoped routes.

   The route data for the selected server or server group appears.

Routes Insert Elements

Table 3-6 describes the elements of the Routes [Insert] form. Elements are displayed for the selected server or server group.

Table 3-6   Routes Insert Elements

Field	Description	Data Input Notes
Route Type	The type of route.	Format: Option
		Range: Net, Default, Host
		Default: N/A
		A value is required.
		Note: The Default route option is available only if there is no default 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: List
		Range: Provisioned devices on the selected server
		Default: N/A
		A value is required.
Destination	The destination network address.	Format: Valid network address
	Note: This field is disabled if the **Route Type** is default.	Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
		Default: N/A
Netmask	A valid netmask for the destination network.	Format: Valid netmask
	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.	Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format
		Default: N/A
Gateway IP	The IP Address of the gateway for the route.	Format: Valid IP address
		Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
		Default: N/A
		A value is required.

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. Click **Configuration**, and then **Networking**, and then **Routes**.

2. Using the tabs, navigate to the target server group or server.

3. Click **Insert**.

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.

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:**
>
> Before editing a route, generate a route report. The route report serves 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. Click **Configuration**, and then **Networking**, and then **Routes**.

2. Using the tabs, navigate to the target server group or server.

   The route data for the selected server or server group appears.

3. Click to select a route and click **Edit**.

   If the route cannot be edited, **Edit** is disabled. If the route can be edited, the Routes [Edit] form 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.

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:**
>
> Before deleting a route, generate a route report. The route report serves 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. Click **Configuration**, and then **Networking**, and then **Routes**.

2. Using the tabs, navigate to the target server group or server.

   The route data for the selected server or server group displays.

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.

   If the route cannot be deleted, **Delete** is disabled. To delete multiple routes at one time, all selected routes must be deletable.

4. Click **Delete**.

   A confirmation box displays.

5. Click **OK** to delete the route.

   The route is deleted.

Generating a Route Report

Use this procedure to generate a route report.

1. Click **Configuration**, and then **Networking**, and then **Routes**.

2. Using the tabs, navigate to the target server group or server.

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 feature allows for flexible network deployment by allowing you to map an application service to a specific network. Additionally, this feature allows for the differentiation of intra- and inter-networks on a per service basis. This means that traffic from different services can be segmented, which allows for service specific-networks and routes. This is predicated on the creation of network elements, networks, and routes to support the segmentation of service traffic.

Geo-redundant (spare) nodes and dual-path monitoring are special code on the node at the spare site that continually monitors the availability of the database instances at the primary site to determine if an automatic failover should occur due to loss of the active site servers. In the event of a network outage, it is possible that if the system is monitoring a single network path only and intra- and inter-networks are differentiated, an erroneous condition might occur where both sites try to assume activity. Inherent dual-path monitoring protects against this scenario.

The core services are:

- OAM
- Replication
- Signaling
- HA_Secondary
- HA_MP_Secondary
- Replication_MP

For example, segregation of replication traffic might occur for inter-network (WAN) traffic only. Prerequisite configuration work would have included the creation of at least one LAN network and two WAN networks along with the related routes. For the purposed of this example, these could be named LAN1, WAN1, and WAN2. The services mapping might look similar to the settings in Table 3-7.

Table 3-7   Core Services

Name	Intra-NE Network	Inter-NE Network
OAM	Unspecified	Unspecified
Replication	LAN1	WAN1
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	LAN1	WAN2

> **Note:**
>
> Services might vary depending on the application. For example, DSR adds a service known as ComAgent to the existing core services. Additionally, workflow and provisioning instruction might differ from the direction provided here. Always follow the provisioning guidelines for your specific application and release.

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. Click **Configuration**, and then **Networking**, and then **Services**.
2. Click **Edit**.
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. Click **OK** to submit the information and return to the Services page, or click **Apply** to submit the information and remain in the Services [Edit] form. Clicking cancel discards your changes and returns you to the Services page.

Generating a Services Report

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

Use this procedure to generate a service reports:

1. Click **Configuration**, and then **Networking**, and then **Services**.
2. Click **Report**.
3. Click **Print** to print the report, or click **Save** to save a text file of the report. Clicking **Back** returns you to the Services page.

Servers

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

- Network OAM&P (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 32 MPs.

- 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

Table 3-8 describes the elements on the Adding a New Server page:

Table 3-8   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 30 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: List Range: Network OAM&P, System OAM, MP, Query Server
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: List of customized options
Network Element Name	The network element must first be set up using the **Configuration**, and then **Network Elements** page.	Format: 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. Typically, this list includes bond interfaces (for example, bond0 and/or bond1). One interface is displayed for each network in the network element.	Format: List

Table 3-8   (Cont.) Add New Server Configuration Elements

Element	Description	Data Input Notes
Interfaces: VLAN	This checkbox allows the user to decide whether to create a VLAN interface.	Format: option
	If the box is checked, a VLAN interface is automatically created. If the box is not checked, the IP address is assigned directly to the interface selected from the list.	
	Only one IP address can be associated with a non-VLAN interface (for example, bond1). One checkbox is displayed for each interface.	
Interfaces: Prefer	Selection of preferred NTP sources, multiple sources can be designated as preferred.	Format: option
	Every NTP Server IP Address field has a corresponding Prefer option.	
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. Click **Configuration**, and then **Servers**.

2. Click **Insert** at the bottom of the table.

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. Click **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. Table 3-9 describes the elements of the Servers Configuration page.

Table 3-9   Servers Configuration elements

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. • MP - Each pair or cluster of servers implementing message processing functions. • 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.

Table 3-9   (Cont.) Servers Configuration elements

Element	Description
Network Element	The name of the network element that is associated with each server. The network element must first be configured using the **Configuration**, and then **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.

Editing a Server

Servers that are currently in-service can be edited but the fields available for edit are limited and vary depending on the role. All servers, regardless of service state, can be edited to add, remove, or change NTP settings. Additionally, on OAM servers, System ID can be changed.

> ⚠️ **Caution:**
>
> Operations, such as NTP sync, should be planned. Critical processes are temporarily shutdown to complete the action. This, or any other in-service operation, should only be run as directed by Oracle support personnel using documentation specific to your application and release.

Use this procedure to edit a server:

1. Click **Configuration**, and then **Servers**.

2. Click to select the server you want to edit.

3. Click **Edit**.

4. Make the desired changes.

5. Click **OK** to save the changes and return to the Servers page. Click **Apply** to submit the changes and remain on the Servers [Edit] form to make additional changes or click **Cancel** to undo the changes and return the values to the previously saved values.

The server edits are submitted to the database.

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. Click **Configuration**, and then **Servers**.

2.   Click to select the server you want to delete.

3.   Click **Delete**.

Click **Yes** to confirm.

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.   Click **Configuration**, and then **Servers**.

2.   Click to select a server to export.

3.   Click **Export**.

The server data is exported to an SH file.

4.   Click Info.

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.   Click **Configuration**, and then **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**, and then **Files** page.

4.   Click **Info.**

5.   Click the **Status and Manage**, and then **Files** link.

The SH files for the server data exported in this procedure is located on the **Status and Manage**, and then **Files** page.

Generating a Server Report

Use this procedure to generate a server report:

1.   Click **Configuration**, and then **Servers**.

2.   Click to select the server for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3.   Click **Report**.

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 NOAM, SOAM, and MP servers. The purpose of this feature is to define database relationships to support the high availability architecture. This relates to replication, availability, status, and reporting at the server level.

From the Server Groups page users can create new groups, edit groups, delete groups, and generate reports that contain server group data. Servers can be added or removed from existing groups using the edit function.

The Server Groups page can be accessed from the main menu by navigating to **Configuration**, and then **Server Groups**. The page displays a grid reflecting all currently configured server groups. A description of the elements displayed in the grid can be found in Server Groups Edit Elements.

> ✎ **Note:**
>
> Depending on the application configuration, the preferred HA role preference, or NE HA Pref, may not be displayed.

Server Groups Insert Elements

Table 3-10 describes the elements of the Server Groups [Insert] form.

Table 3-10   Server Groups Insert Elements

Element	Description	Data Input Notes
Server Group Name	A unique name used to label the server group.	Format: String
		Range: 1-32 characters. Alphanumeric and underscore are allowed. A minimum of one alphabetic character is required and must not start with a digit.
		Default: N/A
		A Value is required.
Level	The level of the servers belonging to this group.	Format: List
		Range: Levels A, B, or C
		Note: Level **A** groups contain NOAMP and Query servers. Level **B** groups are optional and contain SOAM servers. Level **C** groups contain MP servers.
		A Value is required.

Table 3-10   (Cont.) Server Groups Insert Elements

Element	Description	Data Input Notes
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 list.
Function	The defined function for the server group.	Format: List Range: Functions supported by the system
WAN Replication Connection Count	Specifies the number of TCP connections that are used by replication over any WAN connection associated with this Server Group.	Format: Numeric Range = An integer between 1 and 8 Default = 1

Insert a Server Group

Use this procedure to configure a server group:

> **Note:**
>
> Servers are not added at this time. Only after the SG is created can servers be added using the edit function.

1. From the main menu select **Configuration**, and then **Server Groups**.
2. Click **Insert**.
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 list.
5. Select a **Parent** from the list.
6. Select a **Function** from the list.
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. Clicking **Cancel** discards all changes and returns return you to the server groups page.

Server Groups Edit Elements

The Server Groups [Edit] form allows you to edit existing server groups. Table 3-11 describes the elements of the Edit Server Groups page.

Table 3-11   Server Groups Edit Elements

Element	Description	Data Input Notes
Server Group Name	A unique name used to label the server group.	Format: String Range: 1-32 characters. Alphanumeric and underscore are allowed. A minimum of one alphabetic character is required and must not start with a digit. Default: N/A A Value is required.
Level	The level of the servers belonging to this group.	This field cannot be edited. Format: List Range: Levels A, B, or C Note: Level A groups contain NOAMP and Query servers. Level B groups are optional and contain SOAM servers. Level C groups contain MP servers. A Value is required.
Parent	The parent server group that functions as the replication parent of the selected server group.	Format: List **Note**: If the level of the group being inserted is A, then the parent field is not editable and NONE is displayed in the list.
Function	The defined function for the server group.	This field cannot be edited. Format: List Range: Functions supported by the system
WAN Replication Connection Count	Specifies the number of TCP connections that are used by replication over any WAN connection associated with this Server Group.	Format: Numeric Range = An integer between 1 and 8 Default = 1
Prefer Network Element as spare	The Preferred HA Role Setting for the NE. When marked as a preferred spare, the network element only assumes an active or standby role if all the other network elements are unavailable. This allows the user to isolate a dedicated disaster recovery element from normal operations. **Note**: Depending on the application configuration, this selection may not be available.	Format: Checkbox

Table 3-11   (Cont.) Server Groups Edit Elements

Element	Description	Data Input Notes
Server	The name of a server available for inclusion in the server group.	Automatically populated based on servers available for inclusion.
SG Inclusion	When checked, the server is included in the server group.	Checkbox
Preferred HA Role	The Preferred HA Role Setting for the server.	Checkbox
	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. This allows the user to isolate a dedicated disaster recovery node from normal operations.	
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: Four, 8-bit octets separated by periods [The first octet = 1-255; the last three octets = 0-255] Dotted quad decimal (IPv4) or colon hex (IPv6)

Edit 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. Additionally, the edit form presents new fields and choices not present when initially creating the server group. For details regarding specific edit topics, select the appropriate link to display that information.

- For adding a server, see Add a Server to a Server Group.
- For deleting a server, see Delete a Server from a Server Group.
- For assigning a VIP to the server group, see Assign a VIP to a Server Group.
- For removing a VIP from the server group, see Remove a VIP from a Server Group.

Use this procedure to edit a server group:

1. From the main menu select **Configuration**, and then **Server Groups**.
2. From the grid, click to select the server group you want to edit.
3. Click **Edit**.
4. Edit the values you want to change.

    Fields that cannot be edited are 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. Clicking **Cancel** discards all changes and returns return you to the Server Groups page.

Add a Server to a Server Group

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

1. From the main menu select **Configuration**, and then **Server Groups**.

2. From the table, click to select the server group you want to edit.

3. Click **Edit**.

   The Servers Groups [Edit] form 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 is included in the server group.

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. Clicking **Cancel** discards all changes and returns return you to the Server Groups page.

Delete a Server from a Server Group

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

1. From the main menu select **Configuration**, and then **Server Groups**.

2. From the table, click to select the server group you want to edit.

3. Click **Edit**.

4. To delete a server from the server group, de-select the checkbox for **SG Inclusion**. When unchecked, the server is not included in the server group.

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. Clicking **Cancel** discards all changes and returns return you to the Server Groups page.

Assign 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. From the main menu, select **Configuration**, and then **Server Groups**.

2. From the table, click to select the server group you want to edit.

3. Click **Edit**.

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. Clicking **Cancel** discards all changes and returns return you to the Server Groups page.

Remove a VIP from a Server Group

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

1. From the main menu select **Configuration**, and then **Server Groups**.

2. From the table, click to select the server group you want to edit.

3. Click **Edit**.

4. Click **Remove** next to the VIP address you want to remove from the server group.

   The VIP address is removed from the server group.

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. Clicking **Cancel** discards all changes and returns return you to the Server Groups page.

Delete 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 Delete a Server from a Server Group.

1. From the main menu select **Configuration**, and then **Server Groups**.

2. Click to select the server group you want to delete from the table.

3. Click **Delete**.

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

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

Generate a Server Group Report

Use this procedure to generate a server group report:

> **Note:**
>
> Depending on the application configuration, the NE HA Pref, or network element high availability preference, may not be displayed.

1. From the main menu select **Configuration**, and then **Server Groups**.

2. Click to select the server group for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.

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

Table 3-12 describes the elements for adding a resource domain element:

Table 3-12   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
		Default: N/A
Resource Domain Profile	The profile associated with the resource domain.	Format: List
		Range: Policy Binding, Policy Session, and Policy and Charging DRA
Server Groups	The server groups associated with the resource domain	Format: Checkbox
		Range: MPSG, NOSG< SBRSG, SBSG2, SOSG

Insert a Resource Domain

Use this procedure to insert a resource domain:

1. Click **Configuration**, and then **Resource Domains**.

2. Click **Insert** at the bottom of the table.

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.

Edit a Resource Domain

Use this procedure to edit resource domain information

1. Click **Configuration**, and then **Resource Domains**.

2. Select the resource domain from the listing.

3. Click **Edit** at the bottom of the table.

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.

Delete a Resource Domain

Use this procedure to delete a resource domain:

1. Click **Configuration**, and then **Resource Domains**.

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.

Generate a Resource Domains Report

Use this procedure to generate a resource domains report:

1. Click **Configuration**, and then **Resource Domains**.

2. Click to select the resource domain for which you want to create a report.

> **✎ Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.

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

Places

Places are used 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

Table 3-13 describes the elements of the Places Insert page.

Table 3-13   Places Insert Elements

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 of a place group	Format: List
		Note: This field is not used for PCA configuration. The only option is None.
Place Type	The place type.	Format: List
		Range: Site (default option).
Servers	List of the available servers in the NO or SO	Format: Checkbox
		Note: Select all of the DA-MP and SBR servers that are physically located at this Site Place.

Insert a Place

Use this procedure to configure a place:

1. Click **Configuration**, and then **Places**.

2. Click **Insert**.

3. Enter the **Place Name.**

4. Select a **Parent** from the list.

> **Note:**
>
> A Parent Place is not required for PCA Places and can be set as **None**.

5. Select a **Place Type** from the list.

6. Select all of the available DA-MP and SBR **Servers** that are physically located at this Site Place.

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.

Edit a Place

Use this procedure to edit place information

1. Click **Configuration**, and then **Places**.

2. Select the place from the listing.

3. Click **Edit** at the bottom of the table.

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.

Delete a Place

Use this procedure to delete a place.

1. Click **Configuration**, and then **Places**.

2. Click to select the place you want to delete from the table.

> **Note:**
>
> A Place cannot be deleted if it includes servers. Before deleting, disassociate any servers.

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 is not deleted, and you are returned to the Places page.

Generate a Places Report

Use this procedure to generate a places report:

1. Click **Configuration**, and then **Places**.

2. Click to select the place for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold **Ctrl** as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.

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. For PCA, Place Associations are used to identify all sites that require access to the Policy DRA binding database, and to identify sites that share a PCA session database.

Place Association Insert Elements

Table 3-14 describes the elements of the Place Association Insert page.

Table 3-14   Place Association Insert Elements

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: List
		Range: defined by the application
Places	The places available to be grouped in this association.	Format: Option
		Range: list of places defined using Places function

Insert a Place Association

Use this procedure to configure a place association:

1. Click **Configuration**, and then **Place Association**.

2. Click **Insert**.

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

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

4. Optional: Select a **Place Association Type** from the list.

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.

Edit a Place Associations

Use this procedure to edit place associations information

1. Click **Configuration**, and then **Place Associations**.

2. Select the place association from the listing.

3. Click **Edit** at the bottom of the table.

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.

Delete a Place Association

Use this procedure to delete a place association.

1. Click **Configuration**, and then **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 Places. Before deleting the Place Association, disassociate the Places from the Place Association

3. Click **Delete**.

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

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

Generate a Place Associations Report

Use this procedure to generate a place associations report:

1. Click **Configuration**, and then **Place Associations**.

2. Click to select the place associations for which you want to create a report.

3. Click **Report**.

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

DSCP

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

> **✎ Note:**
>
> Use the Differentiated Services Code Point (DSC) pages to configure the priority value of outbound traffic. The router receiving the traffic will use the configured value to prioritize the traffic before sending to the intended destination. The priority value can be applied to a network interface or to a network port of the target. For either case, both TCP and SCTP protocols are supported.

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 Elements

Table 3-15 describes the elements of the Interface DSCP insert page.

> **✎ Note:**
>
> The page tabs and elements reflect your site configuration.

The appearance of the Interface DSCP can vary, and it includes an **Entire Network** tab (when a server group is selected), as well as other server tabs for the selected server group.

Table 3-15   Interface DSCP Elements

Tab/Field	Description	Data Input Notes
Interface/Server	Server groups are presented in tabs at the top of the main work area. Selecting a specific server group reveals the individual servers of that group. Alternatively, selecting the **Entire Network** tab reveals all the servers defined in the system. After selecting a specific server group, the user has the option of selecting a specific server or selecting **Entire Server Group** to reveal the existing routes.	Visible only for the view page.
Interface	The server interface name	Format: List Range: Valid server interfaces
DSCP	DSCP value for the associated network interfaces	Format: Numeric Range: 0 to 63, inclusive Default: NA
Protocol	TCP or SCTP protocol	Format: List Range: TCP or SCTP Default: TCP
Scope (View page only)	The DSCP interface details.	This informational field lists the scope and can reflect the entire network or the scope of one of the configurable container tabs.

Insert an Interface DSCP

Use the following procedure for inserting an interface DSCP.

1. Click **Configuration**, and then **DSCP**, and then **Interface DSCP**.

2. Remain on the tab for Entire Network or select a server group tab.

3. Select a server sub-tab for the interface, or alternatively if a server group tab is selected and the interface is for all servers in the server group select the Entire Server Group sub-tab

4. Click **Insert**.

5. Select the **Interface** from the list of available server interfaces.

6. Enter a valid **DSCP** value. A valid value is an integer between 0 and 63, inclusive.

7. Select **TCP or SCTP protocol** from the list.

8. 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.

Delete an Interface DSCP

Use the following procedure for deleting an interface DSCP.

1. Click **Configuration**, and then **DSCP**, and then **Interface DSCP**.

2. Remain on the tab for Entire Network or select a server group tab.

3. Select a server sub-tab for the interface, or alternatively if a server group tab is selected and the interface is for all servers in the server group select the Entire Server Group sub-tab

4. Click **Delete**.

    A confirmation box appears.

5. Click **OK** to delete the DSCP

Generate 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. Click **Configuration**, and then **DSCP**, and then **Interface DSCP**.

2. Select a server tab or **Entire Network**.

3. Click **Report** to generate a DSCP report. This button generates a report for all the interfaces on the selected server or **Entire Server Group** sub-tab if no rows are selected. If one or more rows are selected, the report only contains the information on the selected rows.

4. Click **Print** to print the report.

5. Click **Save** to save the report to a file.

6. Click **Back** to return to the **Configuration**, and then **DSCP**, and then **Interface DSCP** grid.

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 Elements

Table 3-16 describes the elements of the Port DSCP Insert page.

> ✎ **Note:**
>
> The page tabs and elements reflect your site configuration.

The appearance of the Interface DSCP can vary, and it includes an **Entire Network** tab (when a server group is selected), as well as other server tabs for the selected server group.

Table 3-16   Port DSCP Insert Elements

Tab/Field	Description	Data Input Notes
Port/Server	Server groups are presented in tabs at the top of the main work area. Selecting a specific server group reveals the individual servers of that group. Alternatively, selecting the **Entire Network** tab reveals all the servers defined in the system. After selecting a specific server group, the user has the option of selecting a specific server or selecting **Entire Server Group** to reveal the existing ports.	Visible only for the view page.
Port (Insert page only)	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
Protocol	TCP or SCTP protocol	Format: List
Scope (View page only)	The DSCP port details.	This informational field lists the scope and can reflect the entire network or the scope of one of the configurable container tabs.

Insert a Port DSCP

Use the following procedure for inserting a Port DSCP.

1. Click **Configuration**, and then **DSCP**, and then **Port DSCP**.

2. Remain on the tab for Entire Network or select a server group (but not a specific server for the interface).

3. Select the server for the interface, or alternatively if a server group is selected, create the interface on all servers in the server group by selecting the Entire Server Group tab.

4. Click **Insert**.

5. Enter a valid **Port** value. A valid value is an integer between 1 and 65535, inclusive.

6. Enter a valid **DSCP** value. A valid value is an integer between 0 and 63, inclusive.

7. Select **TCP or SCTP protocol** from the list.

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

Delete a Port DSCP

Use the following procedure for deleting a Port DSCP.

1. Click **Configuration**, and then **DSCP**, and then **Port DSCP**.
2. Select the server or server group containing the interface, alternatively select the **Entire Network** tab.
3. Click **Delete**.
4. Click **OK** to delete the DSCP

Generate 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. Click **Configuration**, and then **DSCP**, and then **Port DSCP**.
2. Click **Report** to generate a report for all DSCPs.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.
5. Click **Back** to return to the **Configuration**, and then **DSCP**, and then **Port DSCP** grid.

4
Alarms and Events

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 Overview

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 disconnected state. Alarms can have these severities:

- Critical application error
- Major application error
- Minor application error
- Cleared

An alarm is considered inactive once it has been cleared and cleared alarms are logged on the **Alarms & Events**, and then **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.

> ✏ **Note:**
>
> Some events may be throttled because the frequently generated events can overload the MP or OAM server's system or event history log (for example, generating an event for every ingress message failure). By specifying a throttle interval (in seconds), the events display no more than once during the interval duration period (for example, if the throttle interval is 5 seconds, the event is logged no more than once every 5 seconds).

Figure 4-1 shows how Alarms and Events are organized in the application.

Figure 4-1   Flow of Alarms
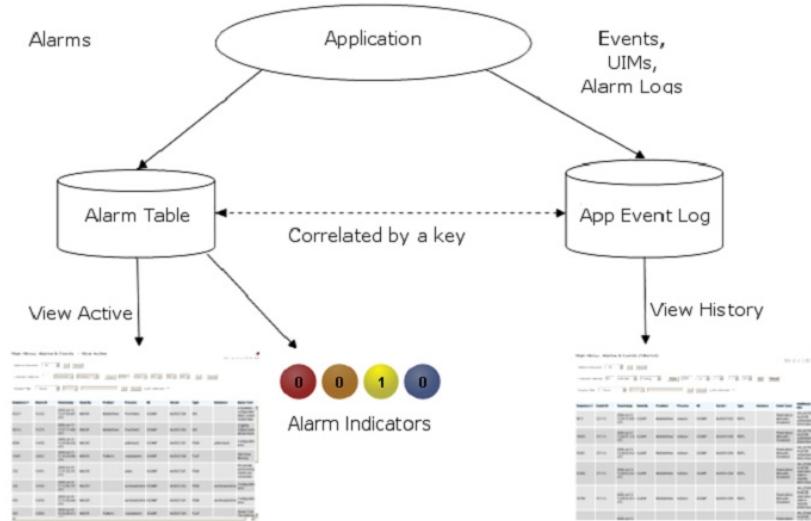
Alarms and events are recorded in a database log table. Application event logging provides an efficient way to record event instance information in a manageable form, and is used to:

• 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. This is shown in Figure 4-2 and Figure 4-3.

Figure 4-2   Alarm Indicators Legend

●	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 4-3   Trap Count Indicator Legend

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

Alarms Formatting Information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of alarm types, see Alarm and Event Types.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm
- Instance: the instance of a managed object for which an alarm or event is generated.

> **Note:**
>
> The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

> **Note:**
>
> Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating that these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

Alarm and Event ID Ranges

The **Alarm ID** listed for each alarm falls into one of the process classifications listed in Table 4-1.

Table 4-1   Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5999
OAM	10000-10999
IDIH	11500-11549
SDS	14000-14999
SS7/Sigtran	19200-19299
Transport Manager	19400-19419
Communication Agent (ComAgent)	19420-19909
DSR Diagnostics	19910-19999
Diameter	8000-8299, 22000-22350, 22900-2999, 25600-25899
Range Based Address Resolution (RBAR)	22400-22424
Generic Application	22500-22599
Full Address Based Resolution (FABR)	22600-22640
PDRA (aka PCA)	22700-22799
SCEF	23000-23200
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32800
DM-IWF	33000-33024
MD-IWF	33050-33099
GLA	33100-33149
Diameter Custom Applications (DCA)	33300-33630
Independent Subscriber Binding Repository (I-SBR)	33730-33830
vSTP	70000-70999
Equipment Identity Register (EIR)	71000-71999

Alarm and Event Types

Table 4-2 describes the possible alarm/event types that can be displayed.

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

Table 4-2   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
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
HTTP	Hypertext Transfer Protocol
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NAT	Network Address Translation
NP	Number Portability
OAM	Operations, Administration & Maintenance
PCRF	Policy Charging Rules Function
PDRA	Policy Diameter Routing Agent
PLAT	Platform
PROC	Process
PROV	Provisioning

Table 4-2   (Cont.) Alarm and Event Types

Type Name	Type
pSBR	Policy SBR
QP	QBus
RBAR	Range-Based Address Resolution
REPL	Replication
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

Active Alarms Elements describes the elements on the View Active alarms page.

Table 4-3   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.
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, for example, Process, Disk, Platform. See Alarm and Event Types for more information.

Table 4-3   (Cont.) Active Alarms Elements

Active Alarms Element	Description
Instance	Instance of the alarm, for example, 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

View 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 NOAM or SOAM. Alarm collection is handled solely by NOAM servers in systems that do not support SOAMs.

1. Click **Alarms & Events**, and then **View Active**.

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

Table 4-4 describes the elements on the **Alarms & Events**, and then **View Active**, and then **Export** form.

Table 4-4   Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once **Note**: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily, and Weekly scheduling options are only available when provisioning is enabled.
Task Name	Name of the scheduled task.	Format: Text box Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. Default: APDE Alarm Export. The default value can only be used once. For scheduled exports, the frequency is not Once, because the name must be unique. **Note**: This field is not active if the selected export frequency is once.
Description	Optional description of the scheduled task	Format: Text box Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character. **Note**: This field is not active if the selected export frequency is once.
Filename Prefix	Optional export filename prefix. The extension to pre-pend the generated export file name.	Format: Text box Range: Maximum length is 8 characters; alphanumeric (a-z, A-Z, and 0-9).
Minute	Select the minute of each hour when the data will be written to the export directory. Enabled only if Export Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list Range: 0 to 59 Default: 0 **Note**: This field is not active if the selected export frequency is Once, Daily, or Weekly. This field is only active if the selected export frequency is Fifteen Minutes or Hourly.

Table 4-4   (Cont.) Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time text box Range: HH:MM with AM/PM Default: 12:00 AM **Note**: This field is not active if the selected export frequency is Once, Fifteen Minutes, or Hourly. This field is only active if the selected export frequency is Daily or Weekly.
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly.	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Export Active Alarms

You can initiate a one-time export task of active alarm data or schedule periodic exports from the **Alarms and Events**, and then **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.

For each export task, the system automatically creates a CSV file of the filtered data. The file is available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the remote server data export feature. For more information about using remote server data export, see Data Export.

Alarm details can be exported to a file by clicking **Export** 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.

Use this procedure to export active alarms to a file, or schedule a periodic data export task of this data.

1. Click **Alarms & Events**, and then **View Active**.

2. Locate and select the server group tab that contains the alarms of interest.

    Server groups are presented in tabular form. If the target server group is not visible in the available screen space, use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.

3. Click **Export**.

4. Select the **Export Frequency**. Based on this selection other fields may become active or inactive.

5. Type a **Task Name**.

    This field is not active if the selected export frequency is once. For more information about **Task Name**, or any field on this page, see Active Alarms Data Export Elements.

6. Optional: Type a **Description**.

   This field is not active if the selected export frequency is once.

7. Optional: Type a **Filename Prefix**.

   The filename prefix is prepended to the generated export file name for quick identification.

8. Select the **Minute** if **Export Frequency** is fifteen minutes or hourly.

   If the selected export frequency is fifteen minutes or hourly, this is the minute of each period when the transfer is set to begin. For an export frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer of the hour.

9. Select the **Time of Day** if **Export Frequency** is daily or weekly.

   This field is not active if the selected export frequency is once, fifteen minutes, or hourly.

10. Select the **Day of Week** if **Export Frequency** is weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, hourly, or daily.

11. Click **OK** to initiate the active alarms export task or **Cancel** to discard the changes and return to the View Active page.

The data export task is initiated or scheduled.
From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

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

• Editing a Scheduled Task

• Deleting a Scheduled Task

• Generating a Scheduled Task Report

> **✎ Note:**
>
> Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export does not start. You must wait until the other export is complete before you can begin your export.

Generate a Report of Active Alarms

Use this procedure to generate a report.

1. Click **Alarms & Events**, and then **View Active**.

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 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.

Graph Active Alarms

The View Active alarm screen includes the ability to produce a set of summary graphs which provide statistical summaries of the active alarms. The active alarms can be graphed based on different topology characteristics or alarm data fields by selecting one or more components from the Graph list. The graphing selections are persistent.

The active alarm graphs display as a series of stacked bar graphs, one bar stack for each server. Each bar stack shows the count of critical, major and minor alarms for the selected items in the Graph list. Multiple graphs display side-by-side for each item selected. The graphs are displayed above the active alarms grid listing.

Use this procedure to graph active alarms:

1. Click **Alarms & Events**, and then **View Active**.

2. If necessary, specify filter criteria In the Filter list and click **Go**.

   The selected Filter criteria are applied to all Server Group tabs. The active alarms that meet the specified criteria display.

3. Specify one or more graphical information components from the Graph list. Valid components are listed in Table 4-5.

Table 4-5   Graphical information components

Topology Components	Alarm Data Field Components
Network Element	Event ID
Server	Severity
Server Group	Product
Resource Domain	Process
Place	Server
Place Association	Type

> **Note:**
>
> Server is both a topology component and a data field in the active alarm data grid display.

The graphs for the selected components display above the tabbed area.

4. To adjust the graph viewing area, click and hold the slider above the graph while adjusting the proportions with the mouse.

5. To remove one or more graphs, de-select the choices from the **Graph** list.

   If only some choices are deselected, the deselected graphs disappear. If all choices are deselected, the graph display disappears.

Active Alarms Quick Filter

The individual information in the bar stacks of the active alarm graphs can be used to further filter the alarm information in the current Server Group tab. This allows a more focused, quick look at the alarms. The quick filter selection(s) are not persistent. The quick filter settings are cleared once the user browses away from the View Active Alarms page.

Quick filter selections from the graph are applied to the grid and all graphs displayed within the current Server Group tab of the View Active Alarms page. For example, if the portion of the stacked bar graph that displays the critical alarms is selected, the grid filters to show critical platform alarms and the summary statistics are recalculated to adjust the graphs. If additional portions of the graphs are selected, both the grid and the graphs continue to be filtered according to the selections.

> **Note:**
>
> Although the quick filter is applied to the grid display, the quick filter criteria are not applied to generated Reports and Exports of active alarm data. Use the **Filter** list in the toolbar to filter the data.

Once active alarms have been graphed, use this procedure to apply a quick filter to active alarms in a server group:

1. To add a quick filter, select a portion of the stacked bar graph to filter. The stacked bar displays lists of active alarms by the alarm severity.

   > **Note:**
   >
   > Alarm severity types are displayed using the following color distinctions:
   >
   > - Critical - Red
   > - Major - Orange
   > - Minor - Yellow

   Upon selection, the filtered graph portion displays green to indicate it is being used as a filter.

2. Repeat the previous step as needed to filter additional portions of the remaining bar graphs.

3. To remove all quick filtering selections from the active Server Group tab, click **Clear Selections**.

   The display grid and all graphs display with no quick filtering.

4. To remove individual quick filtering selections from the active Server Group tab, select the portion of the stacked bar graph that is displayed in green.

   The display grid and all graphs recalculate based on the remaining selections.

View 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 NOAM or SOAM. Alarm collection is handled solely by NOAM servers in systems that do not support SOAMs.

1. Click **Alarms & Events**, and then **View History**.

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 historical 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 alarms and events elements

Table 4-6 describes the elements on the View History alarms and events page.

Table 4-6   Historical Alarms Elements

Historical Alarms Element	Description
Sequence #	A system-wide unique number assigned to each alarm/event.

Table 4-6   (Cont.) Historical Alarms Elements

Historical Alarms Element	Description
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 is appended.
Timestamp	Date and time the alarm/event occurred (fractional seconds resolution).
Severity	Alarm/event severity - Critical, Major, Minor and Info.
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, for example, Process, Disk, Platform. See Alarm and Event Types for more information.
Instance	Instance of the alarm/event, for example, 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.

Historical Events Data Export Elements

Table 4-7 describes the elements on the **View History**, and then **Export** form.

Table 4-7   Schedule Event Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once **Note**: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily and Weekly scheduling options are only available when provisioning is enabled.
Task Name	Name of the scheduled task.	Format: Text box Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. A value is required. **Note**: This field is not active if the selected export frequency is once.
Description	Optional description of the scheduled task	Format: Text box Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). The first character must be alphanumeric. The last character must be a minus sign (-). **Note**: This field is not active if the selected export frequency is once.
Filename Prefix	Optional export filename prefix. The extension to pre-pend the generated export file name.	Format: Text box Range: Maximum length is 8 characters; alphanumeric (a-z, A-Z, and 0-9).

Table 4-7   (Cont.) Schedule Event Data Export Elements

Element	Description	Data Input Notes
Minute	Select the minute of each hour when the data will be written to the export directory. Enabled only if Export Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list Range: 0 to 59 Default: 0 **Note**: This field is not active if the selected export frequency is Once, Daily, or Weekly. This field is only active if the selected export frequency is Fifteen Minutes and Hourly.
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time text box Range: HH:MM with AM/PM Default: 12:00 AM **Note**: This field is not active if the selected export frequency is Once, Fifteen Minutes, or Hourly. This field is only active if the selected export frequency is Daily or Weekly.
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly.	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Exporting Alarm and Event History

You can initiate a one-time export task of alarm history data or schedule periodic exports from the **Alarms and Events**, and then **View History** page. If filtering has been applied in the View History page, only filtered data is exported.

For each export task, the system automatically creates a CSV file of the filtered data. The file is available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the remote server data export feature. For more information about using remote server data export, see Remote Servers.

Use this procedure to export alarm and event history to a file, or schedule a periodic data export task of this data.

1. Click **Alarms & Events**, and then **View History**.

2. Specify the desired filter criteria and click **Go**. The **Collection Interval** is required.

   The alarm and event history files are displayed according to the specified criteria.

3. Click **Export**.

4. Select the **Export Frequency**. Based on this selection, other fields may become active or inactive.

5. Enter a **Task Name**.

   This field is not active if the selected export frequency is once. For more information about **Task Name**, or any field on this page, see Historical Events Data Export Elements.

6. Optional: Enter a **Description**.

   This field is not active if the selected export frequency is once.

7. Optional: Enter a **Filename Prefix**.

   The filename prefix is pre-pended to the generated export file name for quick identification.

8. Select the **Minute** if **Export Frequency** is fifteen minutes or hourly.

   If the selected export frequency is fifteen minutes or hourly, this is the minute of each period when the transfer is set to begin. For an export frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer.

9. Select the **Time of Day** if **Export Frequency** is daily or weekly.

   This field is not active if the selected export frequency is once, fifteen minutes, or hourly.

10. Select the **Day of Week** if **Export Frequency** is weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, hourly, or daily.

11. Click **OK** to initiate the export task or **Cancel** to discard the changes and return to the View History page.

The data export task is initiated or scheduled.
From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

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

- Editing a Scheduled Task
- Deleting a Scheduled Task
- Generating a Scheduled Task Report

> ✎ **Note:**
>
> Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export does not start. You must wait until the other export is complete before you can begin your export. Alarm export times vary based on the number alarms present in the system.

Generate a Report of Historical Alarms and Events

Use this procedure to generate a report.

1. Click **Alarms & Events**, and then **View History**.

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 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

Table 4-8 describes the elements on the View Trap Log page.

Table 4-8   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 display. A link to the report for the record is added if the varbind list is truncated.
Acknowledge All	When **Acknowledge All** 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

Table 4-8   (Cont.) View Trap Log Elements

Element	Description
Acknowledge	selected, the button toggles to **Acknowledge**, and only the selected traps are affected.
Unacknowledge All Unacknowledge	When **Unacknowledge All** 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 **Report All** 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.
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.

View Trap Logs

Trap logs are displayed in a scrollable, optionally filterable table.

1. Click **Alarms & Events**, and then **View Trap Log**.

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 causes 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

Table 4-9 describes the elements on the View Trap Log Report page.

Table 4-9   View Trap Log Report Elements

Element	Description
acked	Indicates whether the trap has been acknowledged. Value = True or False
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 is a varbind entry for each varbind in the logged trap record.

Generate a Trap Log Report

Use this procedure to generate a report..

1. Click **Alarms & Events**, and then **View Trap Log**.

2. Click to select the trap log for which you want to create a report.

> **✎ Note:**
>
> If no trap is selected, the report contains 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**.

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

5
Security Log

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**, and then **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**, and then **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**, and then **Files** page. See Files for steps on how to download files to your computer.

Security Log View History Elements

Table 5-1 describes the elements of the **Security Log**, and then **View History** page.

Table 5-1   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.

View Security Log Files

Use this procedure to view security log files.

1. Click **Security Log**, and then **View History**.

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

Table 5-2 describes the elements on the **Security Log**, and then **View History [Export]** form.

Table 5-2   Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Option
		Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly
		Default: Once
		Note: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily, and Weekly scheduling options are only available when provisioning is enabled.

Table 5-2   (Cont.) Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task.	Format: Text box
		Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must not be a minus sign.
		A value is required.
		Note: This field is not active if the selected export frequency is once.
Description	Optional description of the scheduled task	Format: Text box
		Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
		Note: This field is not active if the selected export frequency is once.
Filename Prefix	Optional export filename prefix. The extension to prepend the generated export file name.	Format: Text box
		Range: Maximum length is 8 characters; alphanumeric (a-z, A-Z, and 0-9).
Minute	Select the minute of each hour when the data will be written to the export directory. Enabled only if Export Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list
		Range: 0 to 59
		Default: 0
		Note: This field is not active if the selected export frequency is Once, Daily, or Weekly. This field is only active if the selected export frequency is Fifteen Minutes and Hourly.
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time text box
		Range: HH:MM with AM/PM
		Default: 12:00 AM
		Note: This field is not active if the selected export frequency is Once, Fifteen Minutes, or Hourly. This field is only active if the selected export frequency is Daily or Weekly.

Table 5-2   (Cont.) Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly.	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Exporting Security Log Files

You can initiate a one-time export task of security log data or schedule periodic exports from the **Security Log**, and then **View History** page. If filtering has been applied in the View History page, only filtered data is exported.

For each export task, the system automatically creates a CSV file of the filtered data. The file is available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the remote server data export feature. For more information about using remote server data export, see Remote Servers.

Use this procedure to export seculogs to a file, or schedule a periodic data export task of this data.

1. From the main menu select **Security Log**, and then **View History**.

2. Specify the desired filter criteria and click **Go**. The **Collection Interval** is required.

   The security log files are displayed according to the specified criteria.

3. Click **Export**.

4. Select the **Export Frequency**. Based on this selection, other fields may become active or inactive.

5. Enter a **Task Name**.

   This field is not active if the selected export frequency is once. For more information about **Task Name**, or any field on this page, see Security Log Data Export Elements.

6. Optional: Enter a **Description**.

   This field is not active if the selected export frequency is once.

7. Optional: Enter a **Filename Prefix**.

   The filename prefix is pre-pended to the generated export file name for quick identification.

8. Select the **Minute** if **Export Frequency** is fifteen minutes or hourly.

   If the selected export frequency is fifteen minutes or hourly, this is the minute of each period when the transfer is set to begin. For an export frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer.

9. Select the **Time of Day** if **Export Frequency** is daily or weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, or hourly.

10. Select the **Day of Week** if **Export Frequency** is weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, hourly, or daily.

11. Click **OK** to initiate the export task or **Cancel** to discard the changes and return to theView History page.

The data export task is initiated or scheduled.
From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

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

•   Editing a Scheduled Task

•   Deleting a Scheduled Task

•   Generating a Scheduled Task Report

> ✎ **Note:**
>
> Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export does not start. You must wait until the other export is complete before you can begin your export.

Generating a Security Log Report

Use this procedure to generate a report.

1. Click **Security Log**, and then **View History**.

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 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.

6
Status and Manage

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

Table 6-1 describes the elements of the **Status & Manage**, and then **Network Elements** page.

Table 6-1   Network Elements Status Elements

Element	Description
Network Element Name	The network element name associated with each server hostname. Each configured network element in the system is listed here.
	A network is a collection of servers that share networking configuration, regardless of physical location or replication relationships.
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. Click **Status & Manage**, and then **Network Elements**.

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 displays a status message. message.

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 2 through 4 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

Table 6-2 describes the elements on the **Status & Manage**, and then **Server** page.

Table 6-2   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** 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

Table 6-3 describes the reporting framework.

Table 6-3   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. Table 6-4 describes the possible alarm severities and their equivalent reporting statuses on the Server page.

Table 6-4   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. Table 6-5 lists the database statuses.

> **Note:**
>
> **Unknown** is the status reported when a failure prevents the reporting or the collection of database status.

Table 6-5   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. Table 6-6 lists the status differences.

> **Note:**
>
> **Unknown** is the status reported when a failure prevents the reporting or the collection of HA availability.

Table 6-6   HA Status versus Reporting Status

| HA Status | Reporting Status Equivalent | | Priority | Color |
	Forced Standby	NOT Forced Standby		
Unknown	Man	Unk	1 (highest)	Red
Offline	Man	Err	Err	2
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. Table 6-7 lists the process statuses.

> **Note:**
>
> **Unknown** is the status reported when a failure prevents the reporting or the collection of process status.

Table 6-7   Process Status versus 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. This is shown in Table 6-8.

Table 6-8   Click-Through Status Screen

Server Status Column	Corresponding Status Page
Alm	Alarm History Page - see View Alarm and Event History
DB	Database Status Page - see Database
HA	High Availability Status Page - see HA (High Availability)
Proc	Processes Page - see Processes

Display Aggregated Server Status

Use this procedure to display a corresponding status page:

1. Click **Status & Manage**, and then **Server**.

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.

Stop 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.

> ⚠️ **Caution:**
>
> 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. Click **Status & Manage**, and then **Server**.

2. Click to select the server you want 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.

Restart 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.

> **⚠ Caution:**
>
> 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. Click **Status & Manage**, and then **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 or process messages.

Reboot 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 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 versus 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.

> **Caution:**
>
> 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. Click **Status & Manage**, and then **Server**.

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.

NTP Sync

Periodically a user has the need to sync or resync one or more servers to the preferred NTP source. This might be required for various reasons including a network change, a new NTP server has been added, or a disaster recovery of an existing NTP server has taken place. Capabilities differ depending on the application. For example, The DSR Network OAM presents a broader scope of eligible servers than the DSR System OAM but the functionality remains the same.

> **Caution:**
>
> This operation should be planned. Critical processes are temporarily shut down to complete the action. The user should understand the concepts of the High Availability (HA) subsystem related to **Max Allowed HA Role**. Reference HA (High Availability).

> **Note:**
>
> **NTP Sync** can only be performed on a server that currently reflects a **Max Allowed HA Role** of Standby, Spare, or Observer.

Use this procedure to perform an **NTP Sync** on one or more servers.

1. Click **Status and Manage**, and then **HA**.

2. Identify the target server(s) on which you want to perform the **NTP Sync** action. Confirm that all target servers reflect a **Max Allowed HA Role** of either Standby, Spare or Observer.

3. Click **Status and Manage**, and then **Server**.

4. Select one or more targets servers and click **NTP Sync**.

   A warning message appears:

   Are you sure you wish to force an NTP Sync on the following server(s)?

5. Click **OK** to continue.

The NTP sync action is invoked on the target server(s). A message is displayed at the top of the work area informing the user of the status of the operation.

Generate a Server Status Report

Use this procedure to generate a server status report on one or more servers . This report differs from the server configuration report in that it presents server status information as defined in the server status elements table. Reference Server Status Elements.

1. Click **Status & Manage**, and then **Server**.

2. Select one or more servers.

> ✏ **Note:**
>
> If no servers are selected then all servers appear in the status report.

3. Click **Report**.

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

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 only occurs 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 shows 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. Table 6-9 describes the details displayed for all servers.

Table 6-9   HA Status Elements

HA Status Element	Description
Hostname	The server's hostname.
OAM HA Role	The operational OAM HA role of 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 for that role.
Application HA Role	The operational application HA role of 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 for that role. • N/A: Not applicable for server.
Max Allowed HA Role	The administrative maximum allowed HA role that the server is allowed to achieve. 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.

Modifying the HA Status

Use this procedure to modify the HA status:

1. Click **Status & Manage**, and then **HA**.

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**, and then **HA**.

Database

The Database page provides:

- The ability to disable and enable provisioning system-wide on the active NOAM 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: disabling and enabling provisioning; displaying a database status report; inhibiting and allowing replication; backing up and restoring database and/or provisioning information; comparing the current database version to a backup to ensure schema compatibility; initiate a manual audit and suspend an automated audit. With the exceptions of restore and replication, these functions affect a single OAM or MP 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. Table 6-10 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 6-10   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. • 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.

Table 6-10   (Cont.) Database Status Elements

Element	Description
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. • 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.

Table 6-10   (Cont.) Database Status Elements

Element	Description
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.

View Database Status

The Database Status page displays a table of all servers and their associated database status. 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:

- Click **Status & Manage**, and then **Database**.

Sort 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).

Generate 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. Click **Status & Manage**, and then **Database**.
2. Click to select the server for which you want to generate a report.
3. Click **Report**.
4. Click **Print** to print the report.

5.   Click **Save** to save the report to a file.

Inhibit/Allow 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 Restore Data to the Active NOAMP Server.

Use this procedure to inhibit replication on a server:

1.   Click **Status & Manage**, and then **Database**.

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 serverserver again, click **Allow Replication**.

Back 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 **Status & Manage**, and then **Tasks**, and then **Active Tasks** 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:**
>
> Depending on the application, the Provisioning button may not be functional. For example, on the active DSR NOAMP, the Provisioning button displays, but it is disabled. The active UDR NOAMP presents the button as functional and the user may toggle the selection as desired.

> **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. Click **Status & Manage**, and then **Database**.

2. Click **Disable Provisioning** and 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**.

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 Tasks box is displayed with the long running task which is managing the backup. You can follow the progress of the backup from the Tasks box. After refreshing the page, 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 this one.

```
Backup on <server_name> status MAINT_CMD_SUCCESS. Success
```

10. Click **Enable Provisioning** and 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**, and then **Files** option to access this file. To transfer the file off-site, use the procedure, Transferring a File to Off-site Storage.

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 are displayed. Table 6-11 describes the elements of the Database Archive Compare page.

Table 6-11   Database Status Elements

Element	Description
SBR Database Compatibility	The compatibility status of the SBR databases being compared.
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.

Table 6-11   (Cont.) Database Status Elements

Element	Description
Contents	The contents of the archived database.
Table Instance Counts	Compares the number of database tables in the current database versus the database archive.

Compare 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 one backup file to do a comparison.

Use this procedure to compare a backed up file with an active database:

1. Click **Status & Manage**, and then **Database**.

2. Click to select the server whose data you want to compare to a backup.

3. Click **Compare**.

4. Click an option to select the backup to compare.

5. 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.

6. Click **Print** to print the report.

7. Click **Save** to save the report to a file.

Restore Data to 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.

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 Transferring a Local File to the File Management Storage Area.

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.

Confirm 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.

Replicate 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. Click **Status & Manage**, and then **Database**.

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. Click **Status and Manage**, and then **Replication**.

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. Click **Status & Manage**, and then **HA**.

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:**
>
> 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. Click **Status & Manage**, and then **Database**.

2. Locate all MP servers.

3. Click **Allow Replication** for each of these servers.

   Replication resumes for each of these servers.

4. Click **Status & Manage**, and then **Replication**.

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. Click **Status & Manage**, and then **HA**.

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.

Enable and Disable Provisioning on the Active NOAMP Server

Use this procedure to enable or disable provisioning updates on the active NOAMP server:

1. Click **Status & Manage**, and then **Database**.

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**.

Enable and Disable Provisioning on the Active SOAM Server

Use this procedure to enable or disable provisioning updates on the active SOAM server:

1. Click **Status & Manage**, and then **Database**.

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

This section provides general information about KPIs, the **Status & Manage**, and then **KPIs** page, and how to view, export, and graph KPIs. Be aware that core KPI functionality is described here. Applications expand on this functionality based on topology and features. Always refer to the documentation for your specific application and release.

KPI Overview

Key Performance Indicators (KPIs) can be accessed from the **Status & Manage**, and then **KPIs** page. KPIs represent point-in-time values monitoring various aspects of system performance. There are two types of KPIs, scalar and arrayed, that are used when the monitored element is either distinct or when the monitored element is repeated. For example, the overall CPU utilization for a system can be monitored as a scalar KPI, and the per core CPU utilization can be monitored as an arrayed KPI (where each array element represents the utilization for a CPU core.)

Two important filter concepts in this section are **Scope** and **Group**. These options can be selected from the **KPI Filter** drawer.

A scope is a collection of servers in a given topology. The scope presented in the first tab is referred to as the Entire Network scope. A sub-scope can be selected from the filter using one of the configurable containers:

• Network Element

• Server Group

• Resource Domain

• Place

• Place Associations

> ✎ **Note:**
>
> Scope is limited to only one selection. Multiple scope selections from the filter are prohibited.

Statistics are calculated across the selected scope. For example, when viewing CPU utilization with a selected scope of **Entire-Network** and a group of **Non Arrayed**, the CPU average statistic displayed is for all CPUs in the topology.

A group is a collection of KPIs. For example, Server, displays various system data related to a server. A group is named, and may consist of any mix of single (scalar) or arrayed KPIs. For presentation, groups are automatically partitioned into sub-groups where all of the scalar KPIs are grouped in the Non Arrayed sub-group, and each

arrayed KPI is grouped into its own sub-group. Applications, topology, and features dictate what named groups are available to the user.

Smooth data presentation is a technique used to provide less erratic updates to the data. This process uses a form a data averaging as opposed to real time data and provides the user with a better overview of what resources are being used.

Exporting of KPIs uses the Automated Performance Data Export (APDE) framework. The export options can be accessed by opening the **KPI APDE Export** drawer. Export tasks can be monitored by opening the **KPI APDE Tasks** drawer. See Exporting KPIs for more information on the exporting of KPIs. See Files for more information on the APDE format.

Graphing options can be accessed by opening the **KPI Graph** drawer. See Graphing KPIs for more on the KPI graphing feature.

KPI work area layout

The KPIs page can be accessed by navigating from the main menu to **Status & Manage**, and then **KPIs**. Notice the title at the top of the work area. Like other pages, the title presents the ordered list of navigation steps taken to reach the current page. The title also reflects the selected group whose information is being displayed in the main work area. An example of this would be:

Main Menu: Status & Manage, and then **KPIs [Group: 'Server']**

In this case the default group of 'Server' is presented in the title bar. This changes as different groups are selected from the filter function.

Unlike some of the other pages viewed in the OAM GUI, the KPIs page uses the concept of drawers. These are similar in function to the **Filter**, **Info**, and **Tasks** lists found on other pages but are located (docked) on the right side of the work area. When selected, they open horizontally presenting the options available.

Under the title bar are two levels of tabs. The top level of tabs present a scope roll-up and subsequent tabs in that row present sub-scoped servers. By default, or when no scope is selected, the view presents a global scope. In this case the first tab is labeled **Entire-Network** and subsequent tabs reflect individual servers. This varies depending on the tier being served by the GUI. Using DSR as an example, the System OAM presents different servers than the Network OAM in the same topology.

The second level of tabs present named groups of arrays with the exception of the first tab. The first tab presents the non-arrayed or scalar KPIs. The subsequent tabs present compatible arrays based on the selected scope.

> **✎ Note:**
>
> The named groups of arrays vary depending on application and features. Refer to documentation specific to your application and release.

KPIs elements

KPI elements vary based on the context of the information being displayed and selected scope. Statistical data is always presented using the smooth data presentation technique. See KPI Overview. Depending on the application, arrayed KPI

names may be pulled from a mapping table providing a proper name. Alternatively, the KPI name may be a simple index and the meaning can be inferred from the context of the group. For example, a multi-core CPU KPI presenting the utilization of each core named 0,1,2,3. Table 6-12 lists the KPI status elements and Table 6-13 lists the KPI statistical elements..

Table 6-12   KPIs Statistical Elements

KPIs Status Element	Description
Name	The KPI name (or index if this is an arrayed KPI without a mapping table).
Average	Average value of the KPI name within the selected scope.
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.
Sum	Summary of all values of the KPI name within the selected scope.
Description	Description of the KPI name.

Table 6-13   KPIs Value Elements

KPIs Status Element	Description
Name	The KPI name (or index if this is an arrayed KPI without a mapping table)
Value	Average value of the KPI name within the selected scope.
Description	Description of the KPI name.

Viewing KPIs

Use this procedure to filter and view KPI data.

By default, the initial page display presents KPI data with a scope of **Entire-Network** and a group of **Non Arrayed**. From this filter set, the work area displays server statistics based on all the servers in this topology. Use this procedure to apply a different filter set and view the corresponding KPI data.

1. From the main menu select **Status & Manage**, and then **KPIs**.

   To isolate the statistics of specific server on the **Status and Manage**, and then **KPIs [Group: 'Server']** page, navigate the tabs in the row containing **Scope** selection tabs. If the target server is not visible in the available screen space use the scroll right/left buttons located to the right or left of the visible tabs in the row containing scope selection tabs.

2. To apply a different filter, select the **KPI Filter** drawer located to the right of the main work area. The filter icon is represented by a funnel. The drawer slides open and presents lists for both **Group** and **Scope**. In addition to the lists, two action buttons are presented: **Go** and **Reset**. Select the desired **Group** and **Scope** and click **Go**.

   The drawer closes and the KPI data displays in the work area. Navigate the **Group** and **Scope** tabs to further isolate the KPI data.

KPIs data export elements

Table 6-14 describes the elements in the Schedule KPI Periodic Export Task drawer.

Table 6-14   Schedule KPI Periodic Export Task Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once **Note**: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily, and Weekly scheduling options are only available when provisioning is enabled.
Task Name	Name of the scheduled task.	Format: Textbox Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. A value is required. **Note**: This field is not active if the selected export frequency is once.
Description	Optional 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. **Note**: This field is not active if the selected export frequency is once.
Filename Prefix	Optional export filename prefix. The extension to pre-pend the generated export file name.	Format: Textbox Range: Maximum length is 8 characters; alphanumeric (a-z, A-Z, and 0-9).
Minute	Select the minute of each hour when the data will be written to the export directory. Enabled only if Export Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list Range: 0 to 59 Default: 0 **Note**: This field is not active if the selected export frequency is Once, Daily, or Weekly. This field is only active if the selected export frequency is Fifteen Minutes and Hourly.

Table 6-14   (Cont.) Schedule KPI Periodic Export Task Elements

Element	Description	Data Input Notes
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time textbox Range: HH:MM with AM/PM Default: 12:00 AM **Note**: This field is not active if the selected export frequency is Once, Fifteen Minutes, or Hourly. This field is only active if the selected export frequency is Daily or Weekly.
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly.	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Exporting KPIs

You can schedule a one-time or periodic export of KPI data from the KPIs page. KPI data can be exported immediately, or you can schedule periodic exports to occur every fifteen minutes, hourly, daily, or weekly.

The **KPI Export** feature uses the Automated Performance Data Export (APDE) framework. See Files for more information on APDE generated files. Once the export task is complete the files can be located in the files management storage area which can be accessed by navigating from the main menu to **Status & Manage**, and then **Files**. The files are 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 Remote Servers.

One or more export files are created for every export task. Exports based on a filtered data set honor scope but not group. All groups are included in the export task. Each exported file contains a unique name with a suffix type of csv. By default the system uses gzip compression. The default compression type can be changed. See Remote Servers for more information.

The csv subgroup portion of the filename is one of the following type:

- SCALAR - the report contains Non-Arrayed items; there is no index column.

- INDEXED - the report contains Arrayed items using a numerical index.

- <map_name> - the report contains Arrayed items using a common name mapped index.

> ✎ **Note:**
>
> Index values can be either numeric or string. For CPU cores, naming the array indexes does not offer any significant value, but for other kinds of arrayed KPIs, the indexes may have a meaningful name (which are used in place of a numeric index.)

Use this procedure to initiate or schedule a KPI data export task.

1. Click **Status & Manage**, and then **KPIs**.

2. Apply the desired filter criteria. Select the **KPI Filter** drawer located to the right of the main work area. The filter icon is represented by a funnel. The drawer slides open and presents lists for both **Group** and **Scope**. Specify filter criteria and click **Go**.

   The KPIs are displayed according to the specified filter criteria.

3. Select the **KPI APDE Export** drawer located to the right of the main work area. The filter icon is represented by a stylistic clock. The drawer slides open and presents the export options.

4. Select the **Export Frequency**. Based on this selection, other fields may become active or inactive.

5. Enter a **Task Name**.

   This field is not active if the selected export frequency is once. For more information about **Task Name**, or any field on this page, see KPIs data export elements.

6. Optional: Enter a **Description**.

   This field is not active if the selected export frequency is once.

7. Optional: Enter a **Filename Prefix**.

   The filename prefix is pre-pended to the generated export file name for quick identification.

8. Select the **Minute** if **Export Frequency** is fifteen minutes or hourly.

   If the selected export frequency is fifteen minutes or hourly, this is the minute of each period when the transfer is set to begin. For an export frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer.

9. Select the **Time of Day** if **Export Frequency** is daily or weekly.

   This field is not active if the selected export frequency is once, fifteen minutes, or hourly.

10. Select the **Day of Week** if **Export Frequency** is weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, hourly, or daily.

11. Click **OK** to initiate the KPI export task.

    KPI export task progress can be monitored from the **KPI APDE Tasks** drawer. See KPI Export Tasks.

The data export task is initiated or scheduled.
From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

Scheduled KPI tasks can be viewed, deleted and reports can be generated from **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**. For more information, see:

• Editing a Scheduled Task

- • [Deleting a Scheduled Task](#)
- • [Generating a Scheduled Task Report](#)

You cannot modify KPIs using this task unless you delete the KPI and create a new one.

> **Note:**
>
> Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export does not start. You must wait until the other export is complete before you can begin your export.

KPI Export Tasks

You can monitor the progress of a **KPI APDE Export** task from the **KPI APDE Tasks** drawer. No task management actions are available from this drawer but active links to the exported files are presented upon selecting a specific task.

Use this procedure to monitor the status of a **KPI APDE Export** task. This procedure assumes an export has been performed or scheduled.

1. Click **Status & Manage**, and then **KPIs**.
2. Select the **KPI APDE Tasks** drawer located to the right of the main work area. The filter icon is represented by a stylistic list. The drawer slides open and presents the task list.
3. To access the active links to exported files select a completed task. The active links appear below the task list and are available for selecting.

   Scheduled and completed tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from the **Status & Manage**, and then **Tasks** page. For more information see:
   - • [Editing a Scheduled Task](#)
   - • [Deleting a Scheduled Task](#)
   - • [Generating a Scheduled Task Report](#)

Graphing KPIs

The graphing function allows for an easy visual display of KPI information over time.

Graph plots the information in selected rows on the grid over time with each line representing a row selected from the grid. A key is displayed to the right of the graph that shows which lines represent which rows.

When only rows of type percentage are selected, the graph displays a range from zero to one hundred on the y-axis. Otherwise, a range from the minimum value to the maximum value (with some buffer) is displayed. The y-axis automatically adjusts if a KPI goes outside the range displayed. When incompatible rows are selected a warning is presented at the top of the drawer stating "Mixed data detected. Results may not be as expected.

Use this procedure to graph KPIs:

1. Click **Status & Manage**, and then **KPIs**.

2. Apply the desired filter criteria. Select the **KPI Filter** drawer located to the right of the main work area. The filter icon is represented by a funnel. The drawer slides open and presents lists for both **Group** and **Scope**. Specify filter criteria and click **Go**.

   The KPIs are displayed according to the specified filter criteria.

3. To isolate the statistics of specific server navigate the tabs in the row containing **Scope** selection tabs. If the target server is not visible in the available screen space use the scroll right/left buttons located to the right or left of the visible tabs in the row containing scope selection tabs.

4. To isolate the statistics of specific group navigate the tabs in the row containing **Group** selection tabs. If the target group is not visible in the available screen space use the scroll right/left buttons located to the right or left of the visible tabs in the row containing group selection tabs.

5. Select one or more lines from the grid representing the desired data set.

   > **Note:**
   >
   > Press **Ctrl** to individually select KPIs. Press **Shift** to select a range of KPIs.

6. Select the **KPI Graph** drawer located to the right of the main work area. The filter icon displays by a stylistic graph. The drawer slides open and displays two action buttons: **Go** and **Reset**. Click **Go** to generate graph.

   The drawer closes and the KPI graph displays in the work area below the KPI grid.

7. To remove the graphing, navigate back to the **KPI Graph** drawer and select **Reset**.

   The drawer is closed and the KPI graph is no longer presented in the work area.

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

Table 6-15 describes elements on the **Status & Manage**, and then **Processes** page.

Table 6-15   Process Status Elements

Process Status Element	Description
Hostname	The hostname of the server.

Table 6-15   (Cont.) Process Status Elements

Process Status Element	Description
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 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.
Heap Memory Used (K)	Size of the heap used per process in Kilobytes.

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 Tasks 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.

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. Table 6-16 describes elements on the Active Tasks page.

Table 6-16   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

Delete a Task

Use this procedure to delete one or more tasks.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

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**.

5. Click **OK** to delete the selected task(s).

Delete All Completed Tasks

Use this procedure to delete all completed tasks.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

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**.

4. Click **OK** to delete all completed tasks.

Cancel a Running or Paused Task

Use this procedure to cancel a task that is running or paused.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

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**.

5. Click **OK** to cancel the selected task.

Pause a Task

Use this procedure to pause a task.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

2. Select a server.

ORACLE®

> **✎ 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**.

5. Click **OK** to pause the selected task.

   For information about restarting a paused task, see Restart a Task.

Restart a Task

Use this procedure to restart a task.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

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**.

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. Table 6-17 describes elements on the Active Tasks [Report] page.

Table 6-17   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

Generate an Active Task Report

Use this procedure to generate an active task report.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

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 is included in the report.

4. Click **Report**.

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:

- Export Active Alarms

- Exporting Alarm and Event History

- Exporting Security Log Files

- Exporting KPIs

- #unique_145

> **Note:**
>
> APDE remote server copy tasks cannot be deleted or edited from the Scheduled Tasks page. The user must perform these actions from the Data Export page.

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. Table 6-18 describes elements on the Scheduled Tasks page.

Table 6-18   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. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

2. Select a task.

3. Click **Edit**.

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. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

2. Select one or more tasks.

3. Click **Delete**.

4. Click **OK** to delete the selected task(s).

Generating a Scheduled Task Report

Use this procedure to generate a scheduled task report.

1. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

2. Select one or more tasks.

> **Note:**
>
> If no tasks are selected, all tasks matching the current filter criteria is included in the report.

3. Click **Report**.

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. Table 6-19 describes the elements on the Files page.

Table 6-19   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 APDE

This table describes the file content types and file name formats for files written to the file management storage area using the Automated Performance Data Export (APDE) framework. APDE defines a common process by which various performance indicators and logs are exported to the file management storage area. These are Alarms, Events, KPIs, Measurements, and Security Logs.

> **Note:**
>
> This section describes the system generated file names only.

In general, APDE generates files with a file name format of:

`<directory path>/<name><suffix><ext>`

Using an example of the type **Events** a file name might look like:

`export/myserver/Events/Events_20159030-112016-EDT_13.csv.gz.`

In this example the **<directory path>** includes `export/<hostname>/<export type>/`. The **<name>** includes `<export type>_<date-time-tz>_<task id>`. The **<suffix>** is `csv` and the **<ext>** is `gz`.

> **Note:**
>
> Depending on the filtering used when the data was exported to the file management area, a scope may be added to the path. This may include a network element or server group.

There are five **export type** categories differentiating the directory paths. We used **Events** in the example but the full list includes:

- Alarms
- Events
- KPI
- Seculog
- Measurements

> **Note:**
>
> The measurements export type is only under the **Measurements** export type directory. The supported types vary according to the measurements offered by the application.

Following the export type in the **<directory path>** comes the **<name>**. With the exception of measurement export file names, the first part of the **<name>** typically begins with the **export type**. Names vary per export type but are similar to:

- `Alarms_<date-time-tz>_<task id>`

- `Events_<date-time-tz>_<task id>`

- `KPI_<date-time-tz>_<task id>`

- `Seculog_<date-time-tz>_<task id>`

- `<Measurements>` have varying name formats which include (but not limited to):

    - `MeasSimple_<date-time-tz>_<task id>`

    - `MeasSimple_<date-time-tz>_<measurement group>_<task id>`

    - `MeasArrayed_<date-time-tz>_<task id>`

    - `MeasArrayed_<date-time-tz>_<measurement group>_<task id>`

    - `<type name>_<date-time-tz>_<task id>`

    - `<type name>_<date-time-tz>_<measurement group>_<task id>`

> **Note:**
>
> Task ID uniquely identifies an individual export task and can be correlated to an active task under **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

By default the `<suffix>` is **csv** (comma-separated value).

The file `<ext>` dictates the compression used and is user defined. The default is gzip. See Remote Servers for details on choosing file compression. Table 6-20 lists the file content types.

Table 6-20   File Name Formats Exports

File Content Type	File Name Common Examples
Exports (APDE)	
Alarms & Events	A common example of an events file is:
	export/<hostname>/Events/Events_<date-time-tz>_<task id>.csv.gz
	A common example of an alarms file is:
	export/<hostname>/Alarms/Alarms_<date-time-tz>_<task id>.csv.gz
	Each of these types are comma-separated value files (csv) compressed using gzip (gz).
Security Logs	A common example of a security log file is:
	export/<hostname>/Seculog/Seculog_<date_time_tz>_<task id>.csv.gz
	Each of these types are comma-separated value files (csv) compressed using gzip (gz).

Table 6-20　(Cont.) File Name Formats Exports

File Content Type	File Name Common Examples
KPIs	A common example of a KPI file is:
	export/<hostname>/KPI/KPI_<date-time-tz>_<task id>.csv.gz
	Each of these types are comma-separated value files (csv) compressed using gzip (gz).
Measurements	Many variations of Measurements files exist. Additionally, the user has the ability to optionally add the measurement group name to the file.
	Some common examples without the measurement group added:
	export/<hostname>/Measurements/OAM.ALARM/MeasSimple_<date-time-tz>_<task id>.csv.gz
	export/<hostname>/Measurements/OAM.SYSTEM/MeasSimple_<date-time-tz>_<task id>.csv.gz
	export/<hostname>/Measurements/OAM.SYSTEM/MeasArrayed_<date-time-tz>_<task id>.csv.gz
	Some common examples with the measurement group added:
	export/<hostname>/Measurements/OAM.ALARM/MeasSimple_<date-time-tz>_<measurement group>_<task id>.csv.gz
	export/<hostname>/Measurements/OAM.SYSTEM/MeasSimple_<date-time-tz>_<measurement group>_<task id>.csv.gz
	export/<hostname>/Measurements/OAM.SYSTEM/MeasArrayed_<date-time-tz>_<measurement group>_<task id>.csv.gz
	Each of these types are comma-separated value files (csv) compressed using gzip (gz).

> **✎ Note:**
>
> It is recommended that policies be developed to prevent overuse of the storage area. These might include a procedure to delete files after transferring them to an alternate location using the data export feature. See Remote Servers for details of the feature.

File Name Formats

This table describes the file content types and file name formats for files written to the file management storage area by processes not using the Automated Performance Data Export (APDE) framework for exporting files. For exports using APDE see File Name Formats APDE for details of those file names.

> **Note:**
>
> Files appearing in the storage area are put there by various automated and manual processes. In some cases the user has the ability to modify the system generated file name. This section describes the system generated file names only.

The file types addressed in this section include:

- **Backup** (Upgrade). This differs from the database backup and is a manual process.
- **Backup** (Database). This differs from the upgrade backup and can be manually or automatically generated.
- **Checkup** (Health Check). These are manually generated files.
- **ISO**. Manually uploaded and system managed.
- **Logs**. These are manually generated files.
- **Servers** (Configuration). These are manually generated files.

The following variables are commonly used in file naming:

- **<server name>** or **<hostname>** is the server hostname from which the file is generated.
- **<checkup type>** is the upgrade health check type. These are EarlyUpgrade, PreUpgrade, or PostUpgrade.
- **<checkup scope>** specifies whether the health check was run on a server group or network element basis.
- **<application name>** is the name of the application.
- **<group name>** is the type of data stored in the backup file.
- **<node type>** specifies whether the backup was generated on an NOAMP or SOAM.
- **<date_time_tz>** is the date, time and time zone that a file was created. This format can vary from file to file. Some may use hyphens while others use underscores. Some files may not include the time zone. The data and time format is generally YYYYMMDD_HHMMSS.
- **<task id>** Task ID uniquely identifies an individual export task and can be correlated to an active task under **Status & Manage**, and then **Tasks**.
- **(AUTO | MAN)** indicates whether the backup was automatically or manually generated.

The various file extensions used are:

- **bz2** is a compressed archive file created by bzip2. This type of file must be uncompressed to access the content inside.
- **gz** is a compressed archive file created by gzip. This type of file must be uncompressed to access the content inside.
- **log** is a flat file type that can be read by a text reader.
- **sh** is a self-extracting archive commonly used in linux systems for scripting.

- **tar** is an archive container and must be unpacked to access the content inside.
- **txt** is a flat file type that can be read by a text reader.

> **Note:**
>
> The file types listed in Table 6-21 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 6-21   File Name Formats

File Content Type	File Name and Description
Backup (Upgrade)	Backup.<application>.<hostname>.FullRunEnv.<group name>.<date_time>.UPG.tar.bz2
	Backup.<application>.<hostname>.FullDBParts.<group name>.<date_time>.UPG.tar.bz2
	Note: In this case the upgrade backup created two files differentiated by run environment and database. Both are tar files separately compressed using bzip2.
Backup (Database)	backup/Backup.<application>.<hostname>.ProvisioningAndConfiguration.<group name>.<date_time>.(AUTO | MAN).tar.bz2
	Note: A database backup can generate files using a default or custom file name. Additionally, the user can select compression or no compression. Available compression choices are bz2 or gz. Files generated using no compression are simple tar files. In this type of backup the user has the choice of Provisioning data, Configuration data, or both
Checkup (Upgrade Health Check)	<checkup type>_HealthCheck_<checkup scope>_<date_time>.txt
	A checkup generates a simple text file that can be viewed or downloaded.
ISO File Image	<name>.iso
	Note: ISO images that have been uploaded but not deployed present a different file name than ISO images that have been uploaded and deployed. For example, an uploaded DSR ISO image has a filename that starts with iso whereas a deployed DSR ISO image has a filename that starts with DSR.
Logs	ugwrap.log
	upgrade.log
	Note: Upgrade or system logs are different than security logs. Seculogs use the APDE framework to export security logs to the file management storage area.
Servers (Configuration)	TKLCConfigData.<hostname>.sh
	Note: Servers configuration data generally starts with the term TKLCConfigData. These are shell files.

> **Note:**
>
> It is recommended that policies be developed to prevent overuse of the storage area. These might include a procedure to delete files after transferring them to an alternate location using the data export feature. See Remote Servers for details of the feature.

View 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**, and then **Files**.

2. Select a server.

   All files stored on the selected server are displayed.

View a File

Use this procedure to view, print, or save the contents of a file in the file management storage area.

1. Click **Status & Manage**, and then **Files**.

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 is disabled, because the contents of tar files cannot be viewed from the GUI.

4. Click **View**.

5. Click **Print** to print the file contents, or click **Save** to save the file.

Upload a File to an Alternate Location

Use this procedure to move a file from the file management storage area to an alternate location.

1. Click **Status & Manage**, and then **Files**.

2. Select a server.

   All files stored on the selected server are displayed.

3. Click **Download**.

4. Click **Save**.

5. Navigate to the drive and folder where you want to save the file.

6. Click **Save**.

Upload 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 My Oracle Support for assistance.

Use this procedure when you want to transfer a local file to the file management storage area:

1. Click **Status & Manage**, and then **Files**.

2. Select a server.

   All files stored on the selected server are displayed.

3. Click **Upload**.

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 appears 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.

Delete 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. Click **Status & Manage**, and then **Files**.

2. Select a server.

   All files stored on the selected server are displayed.

3. Select the file you want to delete.

4. Click **Delete**.

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.

Deploy an ISO File

Use this procedure deploy an ISO file:

1. Click **Status & Manage**, and then **Files**.

2. Select the ISO file.

3. Click **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** list at the top left of the screen.

Undeploy an ISO File

Use this procedure to undeploy an ISO file:

1. Click **Status & Manage**, and then **Files**.

2. Highlight the ISO to be undeployed.

3. Click **Undeploy ISO**.

   A confirmation message displays.

4. Click on the confirmation message.

   The ISO is recalled and is unavailable for upgrade.

Validate an ISO File

Use this procedure to validate an ISO file:

1. Click **Status & Manage**, and then **Files**.

2. Highlight the ISO to be validated.

3. Click **Validate ISO**.

   The ISO is validated. If an ISO image fails validation, it is renamed. An invalid ISO image cannot be deployed.

7

Measurements

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; for example, 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 (NOAM, 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.

Some measurements display as blank (or non-value) and some display as 0. A blank measurement indicates a counter has not been created in the selected reporting

interval. A zero measurement indicates the counter was created, but never pegged. The report may also leave a measurement or sub-measurement out entirely if this item was not created/pegged at all in the reporting interval.

> **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).

> **Note:**
>
> The maximum number of columns displayed in the Measurement report GUI is limited to 150 columns. Export the report to view all columns.

Measurement Elements

Table 7-1 describes the elements on the **Measurements**, and then **Report** page.

Table 7-1   Measurements Elements

Element	Description	Data Input Notes
Report	A selection of reports and the interval of how often the data should cover.	Format: List Range: Varies depending on application Interval: Day, Fifteen Minutes, Five Minutes, Half Hour, Hour Default: None
Scope	Network Elements, Server Groups, Resource Domains, Places, and Place Associations for which the measurement report can be run.	Format: List Range: Network Elements in the topology; Server Groups in the 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

Table 7-1   (Cont.) Measurements Elements

Element	Description	Data Input Notes
Column Filter	The characteristics for filtering the column display.	Format: 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: 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.

> **📝 Note:**
>
> There are number of factors that derive the time taken for exporting the measurements like:
>
> • Measurement groups per export task
>
> • Measurements per Measurement group, whether measurement is arrayed or non-arrayed
>
> • Measurement Pegs
>
> • Number of servers in a topology
>
> • Availability of system resources like CPU and Memory
>
> Refer to Table 7-2 to assess the number of measurement reports generated for each measurement group or scheduled in an export task. For example, an Address Resolution Exception measurement group has single and arrayed measurement types so two measurement reports are generated: one for sing and another for arrayed measurements.

Table 7-2   Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
Address Resolution Exception		Single	5
		Arrayed	15
Address Resolution Performance		Single	4
		Arrayed	21
Application Routing Rules	MeasARTId	Arrayed	1
	MeasApplRoutingRule Id	Arrayed	4
Association Exception		Arrayed	4
Association Usage		Arrayed	1
CAPM	MeasCapmDefId	Arrayed	5
	MeasCapmMeasId	Arrayed	1
	MeasConnectionId	Arrayed	4
CPA Exception		Single	11
		Arrayed	2
CPA Performance		Single	14
CPA Session DB		Single	11
		Arrayed	1
ComAgent Exception	ComAgentHAService ExceptionArrayed	Arrayed	6
	ComAgentHAService ExceptionSingle	Single	1
	ComAgentMeasExcep tionArrayed	Arrayed	1
	ComAgentMeasExcep tionSingle	Single	23
	ComAgentPeerGroup ExceptionArrayed	Arrayed	2
	ComAgentPeerGroup ExceptionSingle	Single	1
	ComAgentPolicerFetc hExceptionArrayed	Arrayed	1
	ComAgentRoutedServ iceExceptionArrayed	Arrayed	17
ComAgent Performance	ComAgentHAService PerformanceArrayed	Arrayed	3
	ComAgentMeasPerfor manceArrayed	Arrayed	2
	ComAgentMeasPerfor manceSingle	Single	15
	ComAgentPeerGroup PerformanceArrayed	Arrayed	2
	ComAgentRoutedServ icePerformanceArraye d	Arrayed	12
Connection Congestion		Arrayed	2

Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
Connection Exception		Arrayed	2
Connection Performance	Egress	Arrayed	24
	Egress Congestion Control	Arrayed	10
	Ingress	Arrayed	7
	Ingress Congestion Control	Arrayed	21
	Message Priority	Arrayed	18
Connection Service		Arrayed	7
Connection Transport		Arrayed	13
DA-MP Exception		Single	2
DA-MP Performance		Single	211
		Arrayed	4
DA-MP Service		Single	2
DAS		Single	14
		Arrayed	1
DCA Framework Exception	DcaDalId	Arrayed	5
DCA Framework Performance	DcaDalId	Arrayed	21
DM-IWF Exception		Single	8
		Arrayed	5
DM-IWF Performance		Single	14
		Arrayed	4
DSR Application Exception		Single	4
		Arrayed	3
DSR Application Performance		Single	14
		Arrayed	5
Diameter EIR Exception		Single	23
Diameter EIR Performance		Single	5
		Arrayed	4
Diameter EIR Usages		Single	31
Diameter Egress Transaction		Single	2
		Arrayed	8
Diameter Exception		Single	3
		Arrayed	6
Diameter Ingress Transaction Exception		Single	3
		Arrayed	10
Diameter Ingress Transaction Performance		Arrayed	8
Diameter Performance		Single	6

Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
	MeasConnectionId	Arrayed	6
Diameter Rerouting		Single	2
		Arrayed	6
Egress Throttle Group Performance		Arrayed	168
Egress Throttle List Performance		Arrayed	167
Full Address Resolution Exception		Single	5
		Arrayed	15
Full Address Resolution Performance		Single	10
		Arrayed	14
GLA Exception		Single	3
GLA Performance		Single	6
HTTP Layer Performance		Single	14
		Arrayed	2
IDIH		Single	7
IPFE Exception	IpfeTotal	Single	2
	IpfeTsa	Arrayed	6
IPFE Performance	IpfeMpServer	Arrayed	6
	IpfeTotal	Single	5
	IpfeTsa	Arrayed	6
License Measurements		Single	15
		Arrayed	14
Link Exception		Arrayed	4
Link Performance		Arrayed	4
Link Set Performance		Arrayed	4
Link Set Usage		Arrayed	1
Link Usage		Arrayed	4
LoadGen Performance		Single	6
MD-IWF Diam Performance		Arrayed	4
MD-IWF Exception		Single	20
MD-IWF Performance		Single	33
		Arrayed	4
MD-IWF SS7 Performance		Arrayed	4
MP Performance		Single	11
Message Priority		Single	16
OAM.ALARM		Single	4
OAM.PERF		Single	17
	Audits	Arrayed	3
	AwSoap	Arrayed	3

Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
	CmSoap	Arrayed	3
	GuiHttp	Arrayed	3
	MmiHttp	Arrayed	3
	TpdSoap	Arrayed	3
OAM.SYSTEM		Single	14
		Arrayed	2
OC-DRA Congestion Exception		Arrayed	1
OC-DRA Diameter Exception		Single	12
		Arrayed	13
OC-DRA Diameter Usage		Single	2
		Arrayed	4
	HistogramMeasBuckets	Arrayed	2
P-DRA Congestion Exception		Single	6
P-DRA Diameter Exception		Single	23
		Arrayed	1
P-DRA Diameter Usage		Single	22
	HistogramMeasBuckets	Arrayed	11
	MeasApn	Arrayed	1
	MeasBuckets	Arrayed	1
	MeasPcrfPool	Arrayed	1
	MeasSubPoolRule	Arrayed	1
P-DRA Site Diameter Usage	MeasSBRuleIncCnt	Arrayed	1
	MeasSBRuleRmvLmt	Arrayed	1
PCA NGN-PS Exception		Single	3
PCA NGN-PS Performance		Single	1
Peer Node Performance		Arrayed	5
Peer Routing Rules	MeasPRTId	Arrayed	1
	MeasPeerRoutingRuleId	Arrayed	4
RD-IWF		Single	7
Route Group Exception		Arrayed	2
Route Group Performance		Arrayed	21
Route List		Arrayed	4
Routing Usage		Arrayed	5
SBR Audit		Single	31

ORACLE

Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
SBR Binding Exception		Single	11
		Arrayed	1
SBR Binding Performance		Single	18
		Arrayed	1
	MeasAltKeys	Arrayed	1
	MeasBuckets	Arrayed	2
	MeasSBRemoval	Arrayed	1
SBR Exception		Single	4
		Arrayed	6
SBR Performance		Single	15
		Arrayed	4
SBR Session Exception		Single	11
	MeasPendingRarDel	Arrayed	1
SBR Session Performance		Single	18
		Arrayed	2
	MeasApn	Arrayed	2
	MeasBuckets	Arrayed	3
	MeasInvokeSisRarType	Arrayed	1
	MeasInvokeSisResult	Arrayed	1
	MeasSessionsRemovedSis	Arrayed	1
SCEF Device Triggering Exception		Single	2
		Arrayed	2
SCEF Device Triggering Performance		Single	12
		Arrayed	25
SCEF ECR Exception		Single	1
		Arrayed	1
SCEF ECR Performance		Single	5
		Arrayed	15
SCEF Exception		Single	13
		Arrayed	1
SCEF Monitoring Exception		Arrayed	3
SCEF Monitoring Performance		Single	5
		Arrayed	91
SCEF NIDD Exception		Single	9
		Arrayed	14
SCEF NIDD Performance		Single	15
		Arrayed	36
SCEF Performance		Single	20
		Arrayed	1

ORACLE®

**Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement
Group**

Report Group	Sub-Group	Type	Number of Measurements
Server Exception		Single	2
Server M3UA Exception		Single	6
Server M3UA Performance		Single	8
Server M3UA Usage		Single	7
Server MTP3 Exception		Single	9
		Arrayed	1
Server MTP3 Performance		Single	4
		Arrayed	2
Server Resource Usage		Single	8
Server SCCP Exception		Single	28
		Arrayed	1
Server SCCP Performance		Single	18
		Arrayed	4
Server TCAP Exception		Single	19
		Arrayed	1
Server TCAP Performance		Single	8
		Arrayed	2
Task Performance		Arrayed	33
Topology Hiding Performance		Single	10
		Arrayed	10
Traffic Throttle Group Performance		Arrayed	23
Traffic Throttle Point Performance		Arrayed	139
Transport Exception		Arrayed	10
Transport Performance		Arrayed	12
Transport Usage		Arrayed	2
USBR Performance		Single	1
		Arrayed	10
VSTP Association Exception		Arrayed	13
VSTP Association Usages		Arrayed	3
VSTP CDPA TT		Arrayed	10
VSTP CGPA TT		Arrayed	10
VSTP Connection		Arrayed	9
VSTP Connection Exception		Single	1
VSTP Connection Performance		Arrayed	10

Table 7-2 (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
VSTP EIR Exception		Single	7
VSTP EIR Performance		Single	27
		Arrayed	1
VSTP LICENSING		Single	4
		Arrayed	2
VSTP LSS Exception		Single	6
VSTP LSS Performance		Single	4
		Arrayed	1
VSTP Link Exception		Arrayed	12
VSTP Link Performance		Arrayed	11
VSTP Link Usage		Arrayed	12
VSTP Linkset Exception		Arrayed	1
VSTP Linkset Performance		Arrayed	7
VSTP Linkset Usage		Arrayed	1
VSTP M2PA Exception		Single	1
	VSTPM2PAException Arrayed	Arrayed	1
	VSTPM2PAException Single	Single	2
	VSTPM2PAException VstpLinkArrayed	Arrayed	14
VSTP M2PA Performance		Single	9
		Arrayed	4
VSTP M3UA Exception		Single	9
VSTP M3UA Performance		Single	4
VSTP M3UA Usages		Single	27
VSTP MNP Exception		Single	11
VSTP MNP Performance		Single	19
		Arrayed	1
VSTP MP Performance		Single	5
		Arrayed	1
VSTP MTP3 Exception		Single	13
		Arrayed	5
VSTP MTP3 Performance		Single	12
		Arrayed	7
VSTP SCCP Exception		Single	7
VSTP SCCP Performance		Single	10

Table 7-2   (Cont.) Number of Measurement Reports for Each Measurement Group

Report Group	Sub-Group	Type	Number of Measurements
VSTP SCCP Usages		Single	1
VSTP Server Exception		Single	5
VSTP Server Usages		Single	4
Vstp MNP Exception		Single	2
Vstp MNP Performance		Single	3

1. Click **Measurements**, and then **Report**.

2. Select the **Measurement Report**.

3. Click **Interval**.

4. Select the **Scope**.

   For details about this field, or any field on the **Measurements**, and then **Report** page, see Measurement Elements.

5. (Optional) Select any filters you may want on the report.

6. Click **Time Range**.

7. Select **Beginning** or **Ending** as the **Time Range** interval reference point.

8. Select the **Beginning** or **Ending** date.

9. Click **Go**.

> **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.

10. To view report data for a specific sub-scope, click on the tab for that sub-scope.

Measurements Data Export Elements

This table describes the elements on the **Measurements**, and then **Report** , and then **Go to Export** page.

Table 7-3   Schedule Measurement Data Export Elements

Element	Description	Data Input Notes
Report Scope	A collection of configurable elements to control report scope.	Format: Options
Report Groups	A graphical list of available groups for report generation.	Format: Options
Time Interval	A configurable element to schedule report generation export frequency.	Format: Options Range: Day, Fifteen Minute, Five Minute, Half Hour, and Hour
Time Range	A configurable element to manage report generation.	Format: Options Range: Days, Hours, Minutes, or Seconds Default: Days
Export Frequency	Frequency at which the export occurs	Format: Options Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once **Note**: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily, and Weekly scheduling options are only available when provisioning is enabled.
Task Name	Name of the scheduled task.	Format: Text box 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	Optional. Description of the scheduled task.	Format: Text box 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	Optional. Frequency at which the export occurs.	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once

Table 7-3   (Cont.) Schedule Measurement Data Export Elements

Element	Description	Data Input Notes
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 text box 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.

> ✎ **Note:**
>
> The maximum number of columns displayed in the Measurement report GUI is limited to 150 columns. Export the report to view all columns.

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**, and then **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**, and then **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**, and then **Tasks** page, you can view a list of files available for download, including the file you exported during this procedure.

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

- Editing a Scheduled Task

- Deleting a Scheduled Task

- Generating a Scheduled Task Report

> **✎ Note:**
>
> The time it takes to generate a single report is based on these factors:
>
> - Number of MPs
>
> - Number of records, for example, data size
>
> - Number of measurement groups/subgroups in a report
>
> - Overall CPU use on the NOAM/SOAM while generating a report
>
> - Number of reports selected
>
> - Frequency of report generation

8
Common Security

The **Common Security**> **Configuration** folder contains the tables to configure the CCNDC Mapping and Neighboring Countries. The pages allow you to view the following information and perform the following actions:

Country Long Lat

A Country Latitude and Longitude is an entry which shows the record of an origin country with its latitude and longitude.

Select the **Common Security**, and then **Configuration**, and then **Country Long Lat** page. The page displays the elements on the **Country Long Lat** View, Insert, and Edit pages.

> ✎ **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 8-1   Country Long Lat Elements

Element	Description	Data Input Notes
Country Name	Name for the country.	Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
Latitude	Defines the latitude of country.	The value will be accurate only upto one digit after decimal.
Longitude	Defines the longitude of the country.	The value will be accurate only upto one digit after decimal.
Mobile Country Code	Mobile Country Code	Minimum: 1, Maximum: 999

You can perform add, edit, or delete tasks on **Common SecurityConfigurationCountry Long Lats** page.

Adding a Country Long Lat

Perform the following steps to configure a new Country Long Lat:

1. Click **Insert**.

> **Note:**
>
> The new Country Long Lat must have a name that is unique across all Country Long Lats at the SOAM. In addition, the Country Long Lat's IP Port combination must also be unique across all Country Long Lats configured at the SOAM.

2. Enter the applicable values.

3. Click **OK**, **Apply**, or **Cancel**

Editing a Country Long Lat

Use this procedure to change the field values for a selected Country Long Lat. (The **Country Long Lat Name** field cannot be changed.):

1. Select the **Country Long Lat** row to be edited.

2. Click **Edit**

3. Enter the updated values.

4. Click **OK**, **Apply**, or **Cancel**

Deleting a Country Long Lat

Use the following procedure to delete a Country Long Lat.

> **Note:**
>
> You cannot delete a Country Long Lat if it is part of the configuration of one or more Linksets.

1. Select the **Country Long Lat** to be deleted.

2. Click **Delete**.

3. Click **OK** or **Cancel**.

CCMCC Map

The Mapping provides the mapping between a Mobile country code and a Mobile network code for network identification.

Select the **Common Security**, and then **Configuration**, and then **CCMCC Map** page. The page displays the elements on the **CCMCC Map** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 8-2   CCMCC Map Elements

Element	Description	Data Input Notes
Country Code	Country codes are short alphabetic or numeric geographical codes (geocodes) developed to represent countries and dependent areas, for use in data processing and communications.	[Min,Max] = [1,999]
Mobile Country Code	Mobile Country Code	[Min,Max] = [1,999]
National Destination Code	National Destination Code identifies the Number Plan Area that is to be used. Default value 0 .	[Min,Max] = [1,999]

You can perform add, edit, or delete tasks on **Common SecurityConfigurationCCMCC Maps** page.

Adding a CCMCC Map

Perform the following steps to configure a new CCMCC Map:

1. Click **Insert**.

> **Note:**
>
> The new CCMCC Map must have a name that is unique across all CCMCC Maps at the SOAM. In addition, the CCMCC Map's IP Port combination must also be unique across all CCMCC Maps configured at the SOAM.

2. Enter the applicable values.

3. Click **OK**, **Apply**, or **Cancel**

Editing a CCMCC Map

Use this procedure to change the field values for a selected CCMCC Map. (The **CCMCC Map Name** field cannot be changed.):

1. Select the **CCMCC Map** row to be edited.

2. Click **Edit**

3. Enter the updated values.

4. Click **OK**, **Apply**, or **Cancel**

Deleting a CCMCC Map

Use the following procedure to delete a CCMCC Map.

> **Note:**
>
> You cannot delete a CCMCC Map if it is part of the configuration of one or more Linksets.

1. Select the **CCMCC Map** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

Neighboring Country

The Neighboring Country is an entry which shows the record of an origin country with its mcc to neighboring country with its neighbor mcc.

Select the **Common Security**, and then **Configuration**, and then **Neighboring Country** page. The page displays the elements on the **Neighboring Country** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 8-3   Neighboring Country Elements

Element	Description	Data Input Notes
MCC	The Mobile Country Code (MCC) is a three digit code that is used in combination with a Mobile Country Code (MCC) to identify a mobile network operator uniquely.	[Min,Max] = [1,999]
Origin Country Name	The name of the origin country.	
Neighboring Country MCC	The Mobile Country Code (MCC) is a three digit code that is used in combination with a Mobile Country Code (MCC) to identify a mobile network operator uniquely.	[Min,Max] = [1,999]
Neighboring Country Name	The name of the neighboring country. Allowed characters are 1 alphabetic character followed by up to 49 alphabetic characters, including spaces.	

You can perform add, edit, or delete tasks on **Common SecurityConfigurationNeighboring Countrys** page.

Adding a Neighboring Country

Perform the following steps to configure a new Neighboring Country:

1. Click **Insert**.

> **✎ Note:**
>
> The new Neighboring Country must have a name that is unique
> across all Neighboring Countrys at the SOAM. In addition, the
> Neighboring Country's IP Port combination must also be unique across
> all Neighboring Countrys configured at the SOAM.

2. Enter the applicable values.

3. Click **OK**, **Apply**, or **Cancel**

Editing a Neighboring Country

Use this procedure to change the field values for a selected Neighboring Country. (The
Neighboring Country Name field cannot be changed.):

1. Select the **Neighboring Country** row to be edited.

2. Click **Edit**

3. Enter the updated values.

4. Click **OK**, **Apply**, or **Cancel**

Deleting a Neighboring Country

Use the following procedure to delete a Neighboring Country.

> **✎ Note:**
>
> You cannot delete a Neighboring Country if it is part of the configuration of
> one or more Linksets.

1. Select the **Neighboring Country** to be deleted.

2. Click **Delete**.

3. Click **OK** or **Cancel**.