Oracle® Communications Network Charging and Control

Service Management System User's Guide

Release 15.2

January 2026

Copyright

Contents

Chapter 12

Using Help 131

About This Document

Scope

The scope of this document includes all functionality a user must know in order to effectively operate the SMS application. It does not include detailed design of the service.

Audience

This guide is written primarily for SMS administrators. However, the overview sections of the document are useful to anyone requiring an introduction.

Prerequisites

Although there are no prerequisites for using this guide, familiarity with the target platform would be an advantage.

A solid understanding of Unix and a familiarity with IN concepts are an essential prerequisite for safely using the information contained in this guide. Attempting to install, remove, configure or otherwise alter the described system without the appropriate skills and knowledge, could cause damage to the system, including:

- temporary or permanent incorrect operation
- loss of service
- unrecoverable damage your system

This manual describes system tasks that should only be carried out by suitably trained operators.

Related Documents

The following documents are related to this document:

- *Service Management System Technical Guide*

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Network Charging and Control (NCC) documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
Italics	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. **Example:** To close the window, either click **Close**, or press **Esc**.
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: **Ctrl+P** or **Alt+F4**.
`Monospace`	Examples of code or standard output.
`Monospace Bold`	Text that you must enter.
variable	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: **Operator Functions > Report Functions**
hypertext link	Used to indicate a hypertext link.

Chapter 1

System Overview

Overview

Introduction

This chapter describes what the Service Management System (SMS) provides and the basic functionality of the system.

In this chapter

This chapter contains the following topics.

Introduction to Service Management System

Description

The Oracle Communications Network Charging and Control (NCC) Service Management System (SMS) provides service management support for existing NCC Intelligent Network (IN) products.

The primary function of the SMS is to provide operators with access to data used by service logic applications.

The SMS provides:

- A central repository for other IN services, such as ACS, CCS
- Generic functions

The SMS main menu provides access to all installed services. To access any service, select the item from this menu.

Functions

SMS provides a number of different support and control functions for other IN applications. The generic functions of SMS include:

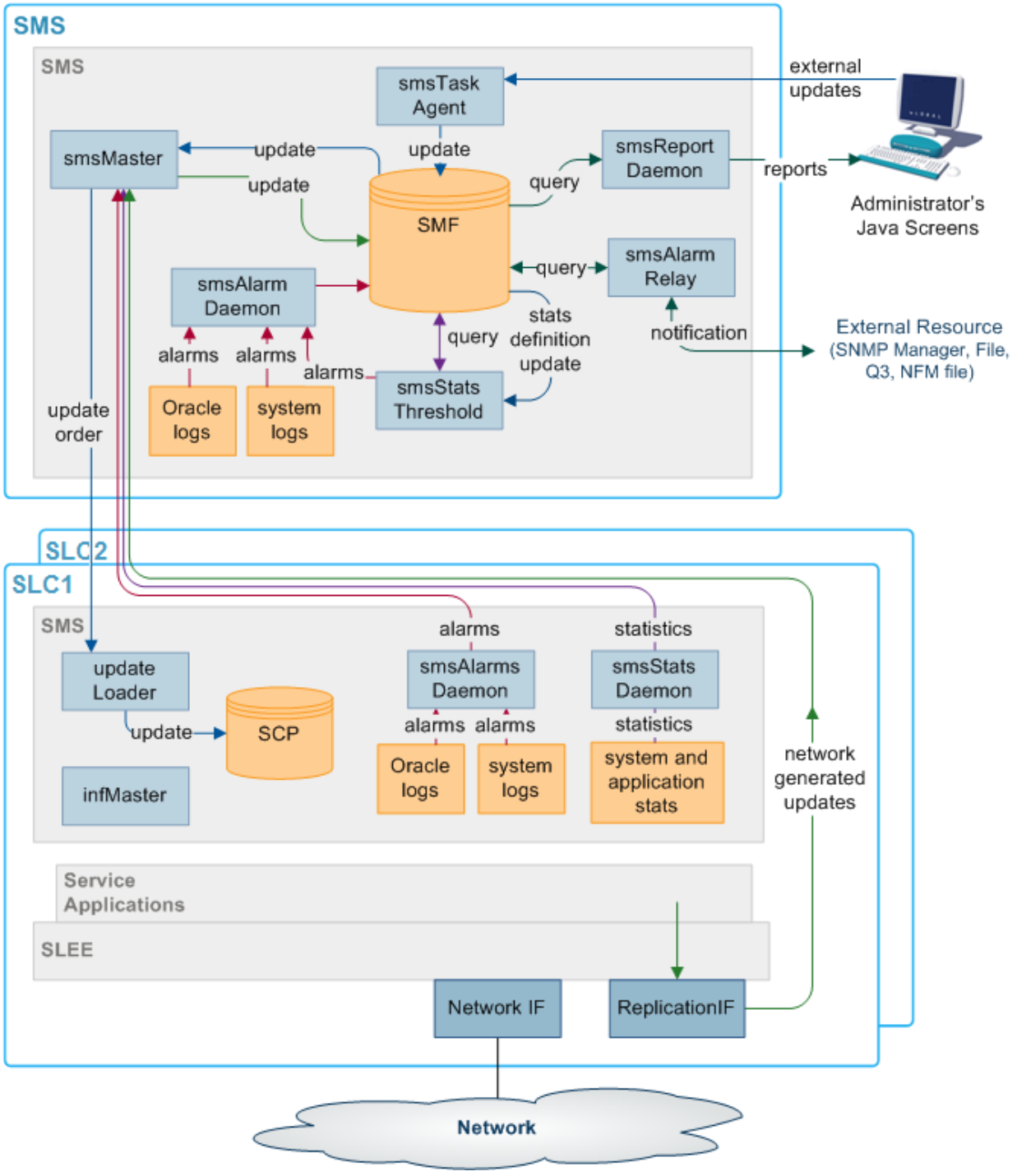
- Replication of configuration and data throughout IN
- Security, users and permissions
- Alarm management and notification
- System and application statistics collection and management
- Report generation and display
- Database changes and replication audits

- smsProcessCdr

Other functions may be added with additional software as necessary. All of these features are discussed later in this guide.

SMS component diagram

Here is an example of the main components of the SMS system.



SMS components description

This table describes the main components in SMS.

Component	Description
smsMaster	The smsMaster process is the superior primary node in the SMS system. It is the central point for replication and manages the SMF database.
SMF database	The SMF database is the central database for the SMS system. It holds all data within the system.
SCP database	The SCP databases are the databases which hold data required for call processing. This is a subset of the data held in the SMF.
updateLoader	The updateLoader processes manage inserting data into the SCPs.
Update Requesters	The Update Requester processes send data update requests to the smsMaster.
smsAlarmRelay	The smsAlarmRelay process forwards alarm notifications to final pick up points for action.
SMS screens	The SMS screens are the Java screens which allow the administrator to interact with SMS.
smsTaskAgent	The smsTaskAgent process receives instructions from the SMS screens and sets up tasks for the smsMaster.
smsAlarmManager	The smsAlarmManager matches alarm instances with the alarm definitions stored in the database, and adds the extra information stored in the definition to each instance of that alarm as it occurs.

Replication Overview

Introduction

Replication is the process that transfers data between points in the IN network. Replication provides:

- Transfer of data between points in the IN network (including configuration and filtering to avoid unnecessary traffic)
- Failover of connections between points and buffering of data to increase resilience
- Recovery from errors

Replication ensures that data is consistent and relevant across the network. Because the SLCs do not require all the data held in the SMF database on the SMS, the SLCs hold restricted sets of that data.

Data transfer requirements are configured automatically when software is installed on the SMS. However, these initial settings can be refined later.

Most error recovery is initiated automatically or from the command line.

For more information about the technical detail of replication (including detailed error recovery and process descriptions), see *Service Management System Technical Guide*.

Nodes

Nodes are points within the IN solution. They are used to identify and locate critical processes in the system and there may be more than one node per machine.

Each node must be configured using the SMS administration screens before it can be part of the IN network.

Nodes include:

- The smsMaster process on SMSs
- The smsMergeDaemon process on the SMS (for unclustered installations)
- updateLoaders on the SLCs
- update requesters.

Replication nodes

A replication node is a node that has data replicated to or from it. Primary replication nodes hold authoritative data that is replicated to other nodes. Primary replication nodes include:

- The smsMaster process on SMSs
- infMaster process on the SLCs (for an unclustered installation)

Other replication nodes include:

- updateLoaders on the SLCs
- Update requesters (which handle alarms, statistics and call processing data)
- The smsMergeDaemon on the SMS (for an unclustered installation)

The replication process

This table describes the stages in the replication process.

Stage	Description
1	An update is one of the following: • Made to the SMF database on the SMS from the SMS Administration screens • Picked up by an update requester and sent to the smsMaster as an update request
2	The smsMaster creates an update order and sends it to all relevant updateLoaders. If the update came from an update requester, the smsMaster returns an acknowledgment.
3	The smsMaster sends update orders to all the update loaders on its replication list.
4	The updateLoaders on each node insert the update information into the SCP database, and send an acknowledgment back to the smsMaster.

Failover

If the smsMaster fails, all other nodes will attempt to connect to the node with the next lowest node number. In a clustered installation, this will be another smsMaster. In an unclustered installation this will be an infMaster process on an SLC. All updates will run to and from the new node until the original smsMaster becomes available. Then the other nodes will return to their original configuration.

For more information about failovers and recovery from a failover, see the *Service Management System Technical Guide*.

Master nodes and the Master Controller

Master nodes manage the authoritative data within SMS and are also known as validators. This is the smsMaster process on the SMS.

The master controller controls all other replication functions that do not start the master replicator. Those functions include:

- Ensuring that all data is consistent
- Merging Master and Inferior Master Replicators (in an unclustered installation)

Security, Users and Permissions

Introduction

SMS provides a system for managing user access to SMS and installed applications. Available functions include:

- Managing user accounts
- Setting passwords
- Creating access rules for different screens and tables within the SMF database

Security levels

SMS supports seven different permissions levels. Starting with level 1, each level has greater permissions up to level 7 - the administrator level. These permissions can be further refined by assigning custom user permission templates.

User permission templates

Permissions can be configured around elements in a SMS screen. Each element can be assigned one of the following permissions:

- Read
- Read and write
- Create and delete
- Access

Elements which can be assigned a specific permission include:

- Screen
- Menu
- Buttons

Once the permissions have been defined in the user template, a specific user can be granted those permissions by having that template assigned to them.

ACS permissions

If ACS is installed, SMS manages the user permissions for that application. For more information about user permissions as they relate to ACS, see *Advanced Control Services Technical Guide*.

Alarms

Introduction

SMS provides a system for:

- Collecting alarms
- Viewing and editing alarms
- Forwarding alarms to notification points for action

The main process involved in collecting alarms is the smsAlarmDaemon.

Filtering alarms

SMS can be configured to filter alarms using a combination of filters that are defined by the user. These filters allow alarms to be filtered as finely as required.

Notification of alarms

Alarms can be reviewed through one of the following:

- The SMS administration screens
- The notification points, including:
  - A file
  - Q3 external resource
  - SNMP external resource
  - NFM external resource

The process responsible for forwarding alarms to the appropriate notification points is the smsAlarmRelay on the SMS.

Further information

For more information about the collection and management of alarms, see *Service Management System Technical Guide*.

Statistics Provided

Introduction

SMS provides a system for managing, configuring and viewing statistics and statistical reports. Some statistics can be set to generate alarms which are forwarded to the alarms management system. The primary process involved is the smsStatsDaemon.

The statistics collected are typically:

- Raw machine statistics (including disk usage, CPU usage, node and process uptime)
- TCAP interface statistics
- Application statistics from the SLEE

Other statistics from applications can be included if they are a compatible format.

Typical statistics values

Typical statistics values might be:

- Total number of requests from SSF
- Number of call instances resulting in error treatment
- Number of calls from invalid geographical locations
- Number of calls reaching successful call completion to international locations
- Number of calls reaching successful call completion to international category one partners.

Further information

For more information about the smsStatsDaemon and how statistics are collected and replicated, see *Service Management System Technical Guide*.

Reports

Introduction

SMS provides reporting functions for installed applications.

Reports can be:

- Generated as needed
- Reused and scheduled to run at specific times

Online reports

Reports are generated to text or html files on the SMS and viewed through the Apache webserver and the SMS Java screens.

Further information

For more information about how to run reports, see *The Report Functions* (on page 109).

For more information about how reports are generated and served through the webserver, see *Service Management System Technical Guide*.

Audit Facilities

Introduction

Replication Checks enable you to check that data is being replicated correctly by comparing the content of two database tables or replication groups.

SMS also provides for auditing of all services that are implemented through it. This keeps track of all changes that are made to the SMF database and saves this information in a database table.

Replication checking

SMS provides tools for checking whether any discrepancies exist between different nodes. If discrepancies exist, a detailed report is produced.

For more information about the replication process and error recovery, see *Service Management System Technical Guide*.

Audit reports

Database change audits are completed using the listAudit.sh tool. For more information about this tool, see *Service Management System Technical Guide*.

Chapter 2

Getting Started

Overview

Introduction

This chapter explains how to access the SMS application and describes the contents of the Main Menu.

In this chapter

This chapter contains the following topics.

Signing on to SMS

To access the SMS user interface (UI), do the following:

Step	Action
1	Ensure the Java SE Runtime Environment version 21 is installed on your machine.
2	If required, obtain, and install the trusted certificate for the database connection into your keystore. Obtain the application zip file containing jars and other files (**smsGui.bat** or **smsGui.sh**) in **/IN/html** directory of SMS Node.
3	In Windows, run **smsGui.bat** to start the application. In other machines: Change the permission of **smsGui.sh** using `chmod 755 smsGui.sh` command. Run the application using `bash smsGui.sh` command. The SMS Login window will appear.

Logging on to SMS

You can log on to SMS using the following two methods:

- Conventional login with OCNCC managed users.
- LDAP based login. For more information about how to configure LDAP based login, see *Service Management System Technical Guide*.

Follow these steps to log on to SMS using conventional login method.

Step	Action
1	On the SMS Login screen:  Enter a user name.
2	Enter the password. **Note:** Passwords are case-sensitive.
3	Click **OK**.

Follow these steps to log on to SMS using LDAP based login method.

Step	Action
1	On the SMS Login screen, select the **Use LDAP Account** checkbox. **Note**: If this checkbox is not selected, the conventional login method is followed.
2	In the **User Name** field, enter your LDAP user ID.
3	In the **Password** field, enter the LDAP password. **Note:** Passwords are case-sensitive.
4	In the **DB Password** field, enter the LDAP DB user password. This is the password created for LDAP_DB_USER. For more information about LDAP_DB_USER, see *Service Management System Technical Guide.* **Note**: This field is enabled only when the **Use LDAP Account** checkbox is selected.

5 Click **OK**.

You have three attempts to enter a correct user name and password before the User ID is locked. If this happens, you must see your system administrator to re-activate the account.

SMS Main Screen

Main Screen

Here is the Service Management System main screen.

The menu bar at the top of the screen provides access to all the functional components of the SMS application.

Available menus

There are four menus available on the Service Management System main screen.

Menu	Description
File	Provides the system options such as logging off the system. **Notes:** • Exiting SMS closes the browser set for that instance of SMS. Do not exit SMS or close the browser window until you have finished using the software. • To keep your browser window open when you close SMS, select **File>Logout**. This allows you to subsequently login as the same user on the next login attempt. You can restart the screens by refreshing the web browser. • To log in as a different user, select **File>Logout & Exit** and restart the web browser.
Services	Provides access to the services installed on the SMS. Services may include: • ACS Service

Menu	Description
	• Prepaid Charging Service For more information about how to use these services, see the User's Guide for that service.
Operator Functions	Provides the main SMS screens described in this User's Guide.
Help	Provides version and copyright information about the SMS. **Note:** To access context sensitive help about the screen or tab that you have open, click the **Help** button on that screen. For more information, see *Accessing Help* (on page 131).

Selecting Languages

Supported Languages

All screens in the SMS support selected languages. On login, the screens display the default language.

You may select a different language for a user in the **Configuration** field of the User Management screen. The selection is stored in the user's profile. Select the language from the list of available language files.

Adding a language

To add a language to the range available, take a copy of the lang. file in the language directory for the service (for example, /IN/html/sms/language directory/eng.lang) and rewrite the (English) strings into the required language. Save the file into the language directory.

Using the Find Screens

Introduction

A find screen enables you to find records that match the selection criteria. All find screens in the system contain the following areas:

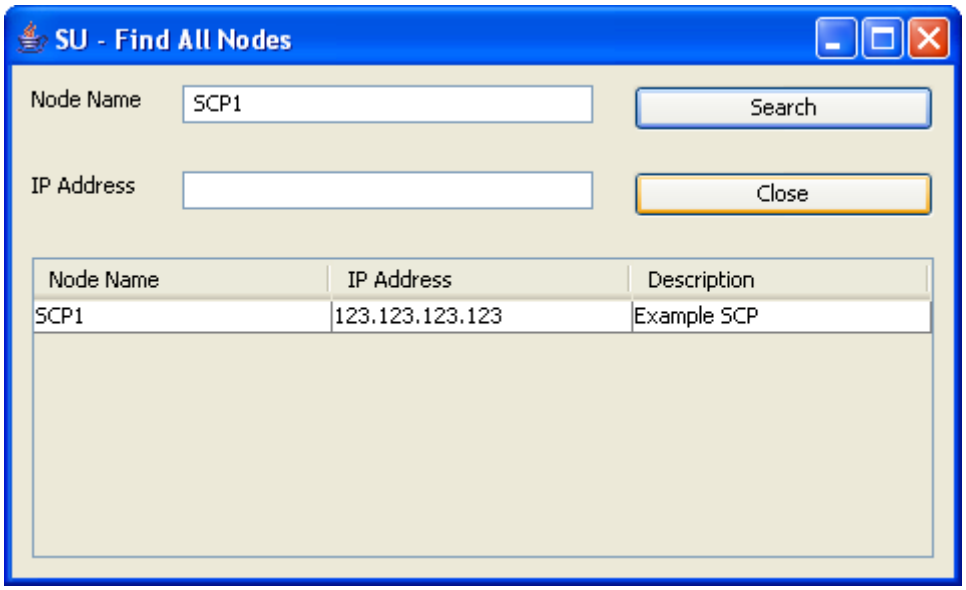
- Buttons
- Query fields
- Display grid

Accessing a find screen

To access the context sensitive find screen for a screen or tab, click **Find**.

Example SMS find screen

Here is an example find screen.



The top half of a find screen provides the query fields and the lower half lists the results of the search.

Searching the database

Follow these steps to search the database.

Step	Action
1	Enter selection criteria in one or more query fields at the top of the screen and click **Search**. If a field is left empty, the search retrieves all instances of that field. **Result:** This triggers an Oracle Like% query that returns the first 100 records that begin with the selection criteria. These are displayed in the display table at the bottom of the screen. **Example:** If you enter 123 in a query field, the system returns records such as 123, 1234, and 12345. **Note:** These are the first 100 records entered in the database, and they display in no particular order. If you do not find the record you are searching for, you need to conduct a more specific search.
2	To display the record in the main screen, select the record line and click **Close**.

Using Keyboard Shortcuts

You can use keyboard shortcuts for many actions in SMS GUI.

Action	Shortcut
To open **File** menu on the **Service Management System** screen.	Alt + F
In a drop-down menu, move to the next item in the list.	Down Arrow
In a drop-down menu, move to the previous item in the list.	Up Arrow

Action	Shortcut
In a drop-down menu, to expand the sub-listed items (mentioned with >).	Right Arrow
To enter the selected item from the drop-down list.	Enter
To traverse to menus other than the **File** menu on the **Service Management System** screen.	Right or Left Arrow
To traverse through the tabs of a screen.	Ctrl + Tab
To traverse forward to the forms or fields of a selected tab of the screen.	Tab
To traverse backward to the forms or fields of a selected tab of the screen.	Shift + Tab
To toggle between the radio buttons in the same row.	Right or Left Arrow
To click the button on focus.	Enter
To enable or disable the selected check box or radio button.	Spacebar
To select value from the drop-down list of values for a field.	Up or Down Arrow

Chapter 3

Initial Configuration - Node Management

Overview

Introduction

This chapter explains how to configure the SMS for the first time. It assumes that you have already installed the SMS software on all of the SLCs you will use.

For information about installing the software, see the *Service Management System Technical Guide*.

In this chapter

This chapter contains the following topics.

Node Management Module

Introduction

The Node Management screen is used to set up the nodes used in SMS. It contains these tabs:

- *All Nodes* (on page 16)
- *Replication Nodes* (on page 19)
- *Table Replication* (on page 23)

Each of the following must be set up as nodes before they can be used:

- Each SMS
- All SLCs (in an unclustered installation)
- All updated loaders

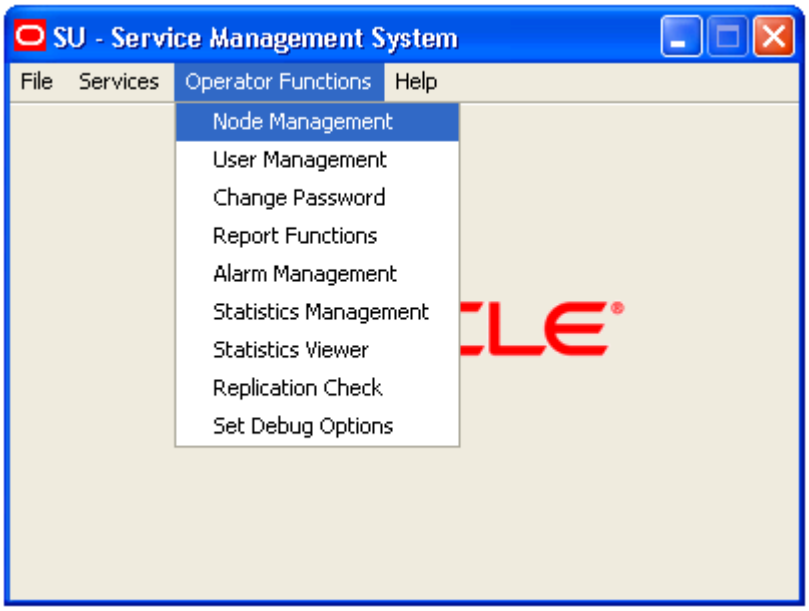
Note: The SMS nodes are set up when the software is installed. All other nodes must be configured separately.

Accessing the Node Management screen

Follow these steps to access the Node Management screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



2 Select **Node Management**.

Result: You see the Node Management screen.

All Nodes

Introduction

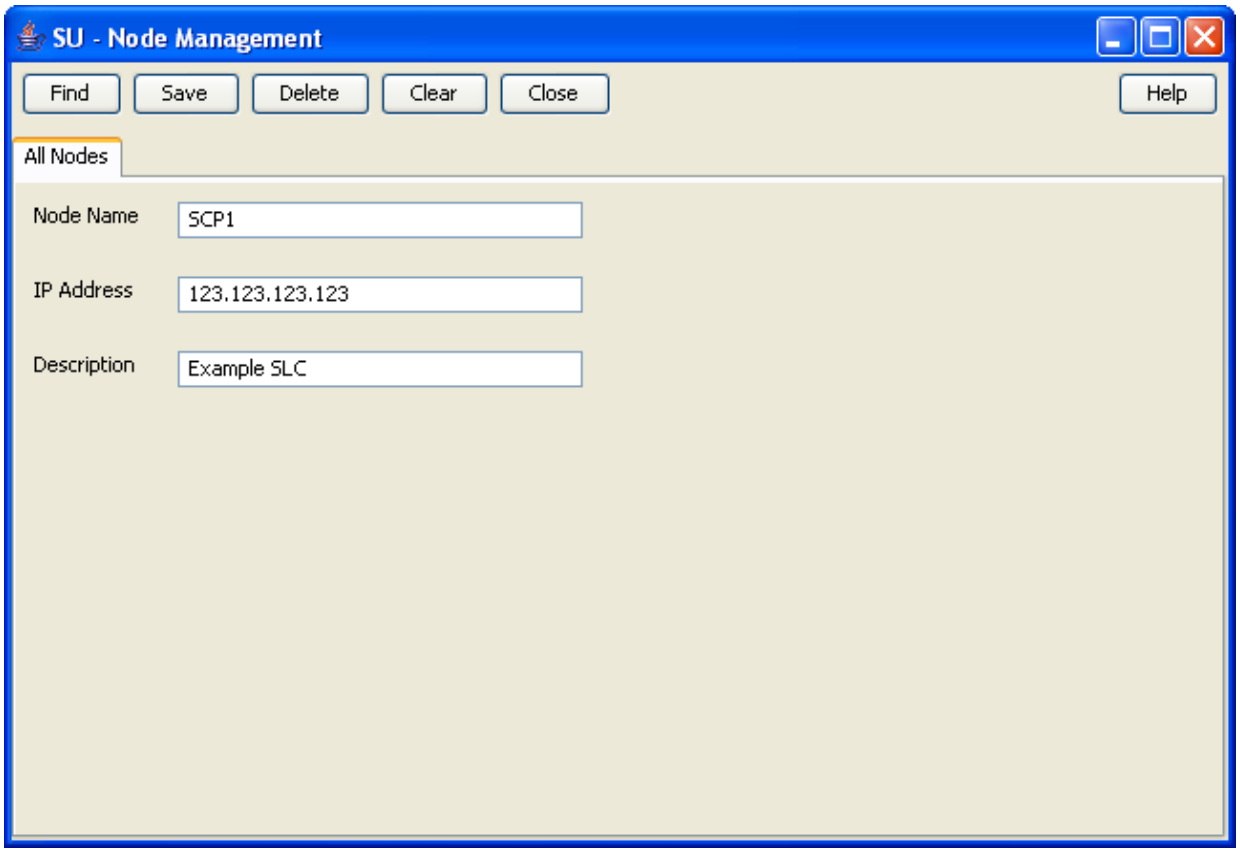
The **All Nodes** tab of the Node Management screen enables you to add, modify, or delete nodes.

The SMS installation process automatically adds the SMS nodes. However, you must manually add the node name and address for each SLC.

Note: When you add a new node, you must ensure that the node name exactly matches the host name. If the names do not match, then the statistics viewer will be unable to display statistics about the node.

All Nodes tab

Here is an example **All Nodes** tab.



All Nodes fields

The table below describes the function of each field.

Field	Description
Node Name	Name of the node, which can include the name of an SLC. This field is a maximum of 10 alphanumeric characters and is compulsory.
IP Address	IP address where the Node is located. Format includes one of the following: • Four octets separated by periods (for example: 123.123.123.123.) • Platform name This field is compulsory.
Description	Description of the node. This field is a maximum of 50 alphanumeric characters and is optional.

Adding a node

Follow these steps to add a new node. Repeat this procedure for each SLC on the system.

Step	Action
1	If the fields on the **All Nodes** tab are populated with node data, click **Clear**.

Step	Action
2	In the **Node Name** field, enter the name of the new node (required). **Note:** To ensure you can view statistics for the node, the node name must match the host name exactly.
3	In the **IP Address** field, enter the IP address of the node (required).
4	In the **Description** field, enter a description of the node (optional).
5	Click **Save**. **Result:** The new Node details are saved to the database.

Changing a node

Follow these steps to change a node.

Step	Action
1	On the **All Nodes** tab, find the required node. See *Using the Find Screens* (on page 12).
2	Change the details of the node as required. **Note:** If you change the IP address of the node, you will create a new node. The original node will remain.
3	Click **Save**. **Result:** The changes will be saved to the database.

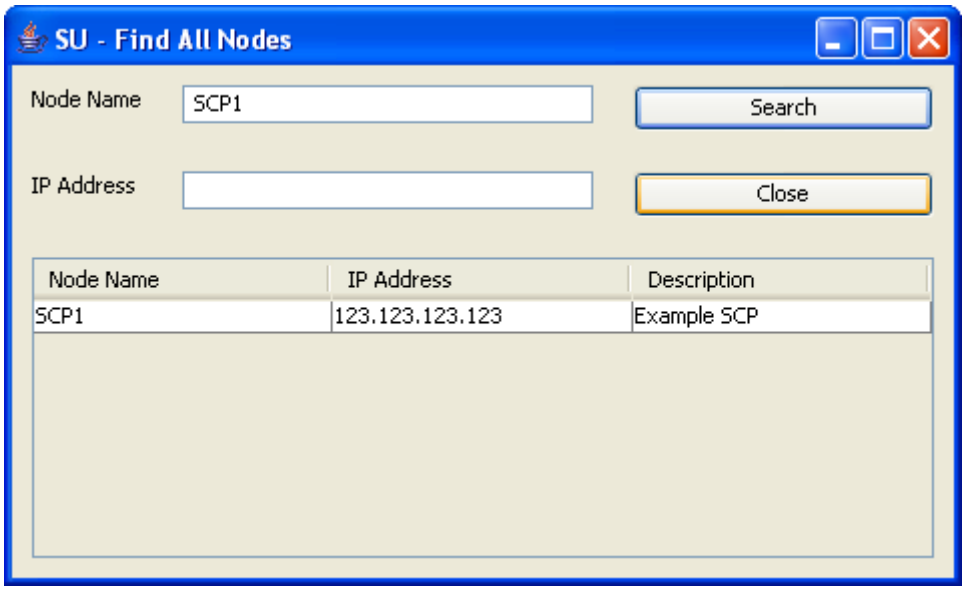
Deleting a node

Follow these steps to delete an existing node record.

Step	Action
1	On the **All Nodes** tab, find the required node. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** You will see a delete confirmation prompt.
3	Click **OK**. **Result:** The record will be deleted from the database. **Note:** You cannot delete a node if there are references to it within SMS.

Find All Nodes screen

Here is the Find All Nodes screen.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Replication Nodes

Introduction

The **Replication Nodes** tab enables you to add, modify and delete nodes used in replication.

The SMS installation process automatically adds the SMS replication nodes. However, you must manually add the replication node for each SLC.

Replication Nodes fields

The table below describes the function of each field.

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td rowspan="6">Node Number</td><td colspan="2">Unique identifier for each node.
Nodes are elements of the replication system and which are replicated (copied) to or from. There can be more than one node per platform.
The allocation of node numbers must follow the rules below:</td></tr>
<tr><td>Number</td><td>Description</td></tr>
<tr><td>1-255</td><td>These numbers are reserved for the master nodes. 1 must be given to an smsMaster. 2-255 will be assigned to smsMasters in a clustered installation and infMasters in an unclustered installation.</td></tr>
<tr><td>256 – 511</td><td>Update loaders on SLCs</td></tr>
<tr><td>> 511</td><td>Must not enter node numbers greater than 511</td></tr>
<tr><td colspan="2">This field is compulsory.
For more information about nodes, see Service Management System Technical Guide.</td></tr>
<tr><td>Primary Node IP Address</td><td colspan="2">List of available primary node IP addresses or platform names.</td></tr>
<tr><td>Secondary Node IP Address</td><td colspan="2">List of available secondary node IP addresses or platform names.
Note: Do not specify a secondary name if replication is performed on a single platform.</td></tr>
<tr><td>Description</td><td colspan="2">Description of the node.</td></tr>
<tr><td>Validator</td><td colspan="2">This check box indicates that the replication node is an smsMaster replication node. Only replication nodes on SMSs may be validators.
A validator has a complete database that can replicate validated updates.
Do not select this option if the platform is a SLC.</td></tr>
</table>

Checking the SMS Replication Nodes

Check each SMS node has all of the following:

- Valid primary address (or hostname)
- **Node Number** of 1-16 (there must be at last one SMS node with 1 as its node number)
- **Validator** option selected

Checking the SLC Replication Nodes

Each SLC has two node numbers associated with it:

- One in the range 17 to 255 for the inferior master (in an unclustered configuration)
- One in the range 256 to 511 for the update loader.

Each inferior master should have:

- Valid primary address (or hostname)
- **Node Number** in the range 17 to 255
- Empty **Validator** option.

Each update loader should have:

- Valid primary address (or hostname)
- **Node Number** in the range 256 to 511 (the node number of update loaders should start with 301 and work upwards)
- Empty **Validator** option.

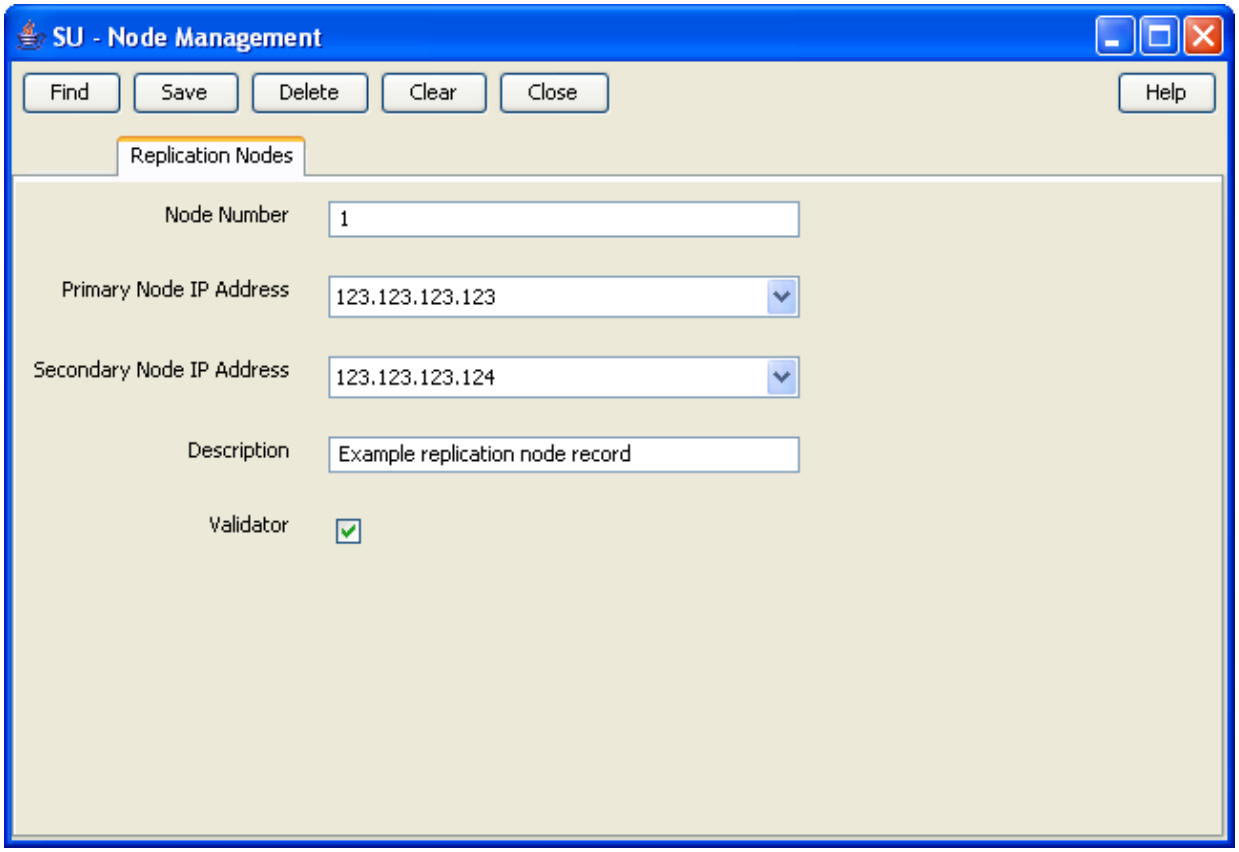
Adding a replication node

Follow these steps to add a new replication node. Repeat this procedure for each SLC on the system.

Step	Action
1	If the fields on the **Replication Nodes** tab are populated with node data, click **Clear**.
2	In the **Node Number** field, enter the number of the node.
3	From the **Primary Node IP Address** drop down box, select the IP address for the primary node.
4	If you will be replicating on more than one platform, select the secondary node from the **Secondary Node IP Address** drop down box.
5	In the **Description** field, enter a description of the replication node.
6	If this replicator node is an smsMaster, select the **Validator** check box. In all other circumstances ensure the **Validator** check box is deselected.
7	Click **Save**. **Result:** The details will be saved to the database.

Replication Nodes tab

Here is an example **Replication Nodes** tab.



Changing a replication node

Follow these steps to change a replication node.

Step	Action
1	On the **Replication Nodes** tab, find the node to edit. See *Using the Find Screens* (on page 12).
2	Change the details of the node as required.
3	Click **Save**. **Result:** The changes are saved to the database.

Deleting replication nodes

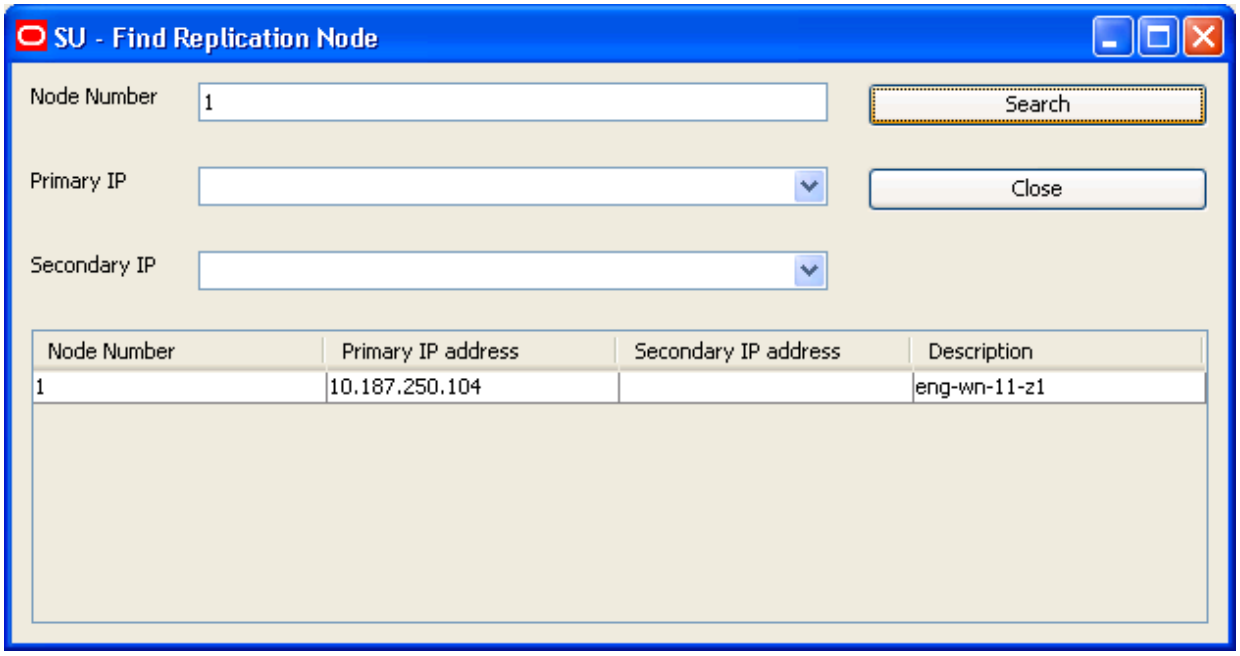
Follow these steps to delete an existing replication node.

Step	Action
1	On the **Replication Nodes** tab, find the node to delete. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The confirmation prompt will appear.
3	Click **OK**. **Result:** The record will be deleted from the database.

Note: You cannot delete a node if there are references to it within the SMS.

Find Replication Node screen

Here is an example of the **Find Replication Node** screen.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Table Replication

Introduction

The **Table Replication** tab of the Node Management screen enables partitioning database replication groups onto physical nodes.

You can specify which table groups will be replicated from a particular node. The table groups are displayed in the left window while the nodes are displayed in the right window. The replication group list displayed is customized to a specific node. No group information is displayed until a node is selected. The group information is customized to a particular node by the annotation of table groups already added to the replication nodes list.

A table group already allocated to the node is indicated as, "—`added to node`—" and cannot be reallocated to the same node.

Multiple groups or a block of groups may be selected simultaneously at table, module or application root level. However, this requires the assignment of a 'filter' to the add operation.

SMS checks for resource dependencies and will notify you if there are any conflicts.

Filters

A filter allows certain preselected table groups to be extracted from a block-selection. This is essential as a block-selection will select all the table groups from any table having multiple table groups, whereas only one may be selected per table.

Filters are used to define node types which allow block-creation of nodes identical in terms of their replication groups.

Dependencies

When allocating replication groups to nodes, either as block selections or individual sub-groups, it is important to note any inter table dependencies.

A dependency arises when a table has a foreign key from another table. This requires that both tables must be selected for replication. The tables may be selected at the same time and need not be selected in any particular order. If a dependency is not fulfilled, the User will be prompted to add it to the selection retroactively.

Table Replication tab

Here is an example **Table Replication** tab.

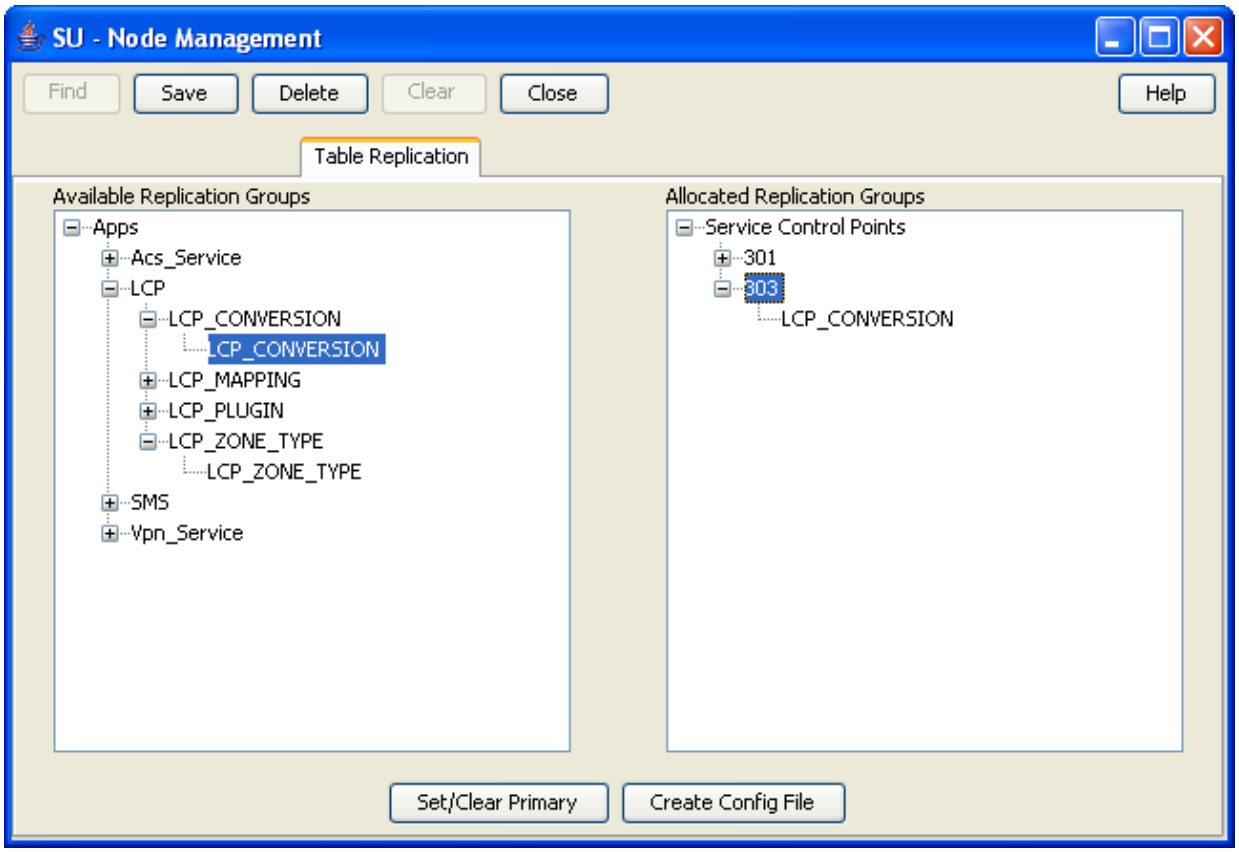


Table Replication fields

This table describes the function of each field.

Field	Description
Available Replication Groups	Displays a list of available groups for replication.
Allocated Replication Groups	Displays a list of available nodes for allocating the replication table groups.

Replication groups

A replication table has one or more replication groups. A replication group can be assigned to one or more replication nodes.

Example:

- Replication Group A resides on Node 1, Node 2 and Node 3
- Replication Group B resides on Node 1 and Node 3

Primary replication nodes

Primary nodes can be defined for a specific replication group. The primary is the highest priority destination node for the data defined in the replication group. This enables the IN to assign particular services to specific nodes, but still provide a failover to other nodes as required.

This only sets the node as the primary for the specific group involved and is independent of other groups. A node may be defined as a primary for one group without being a primary for another group.

Example:

- Replication Group A resides on Node 1, Node 2 and Node 3, where Node 3 is the primary for group A.
- Replication Group B resides on Node 1 and Node 3, where Node 1 is the primary for group B.

Primary nodes are not required unless a service is running with different priority on different nodes.

Table Replication buttons

This table describes the function of each button specific to this screen.

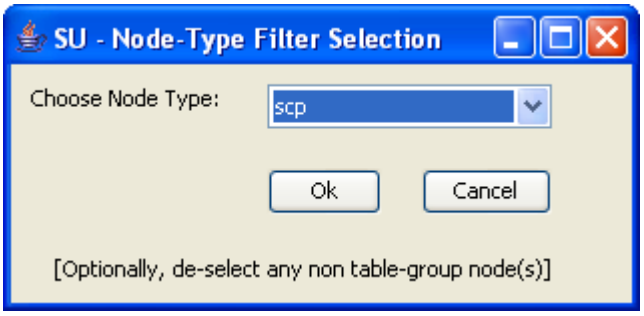
Button	Description
Set/Clear Primary	Use to set or clear the allocation of the node as primary for the replication group. Primary nodes are a logical setting used in information management. Primary nodes are the primary destination to which data is replicated. If the primary node fails, the secondary node will act as a backup. **Example:** There are 2 SLCs and two services. Service 1 normally runs on SLC1 (primary node). SLC2 acts as a hot standby node, in case SLC1 fails.
Create Config File	This button overwrites the existing replication configuration file on the SMS, with the new data entered. It then updates the replication configuration files on all replication nodes. **Note:** This button will fail to copy the replication configuration file to any node which has not had its ssh keys correctly configured. For more information about configuring ssh keys, see *Service Management System Technical Guide*.

Allocating a replication group

Follow these steps to allocate a new replication group using the Table Replication tab.

Note: You can also use the *Replication Node Types* (on page 28) tab to allocate replication groups.

Step	Action
1	On the **Table Replication** tab, click **Clear**.
2	Expand the tree in the **Allocated Replication Groups** box to the required node name and select it.

Step	Action
	Result: The group list specific to the selected node will be displayed in the **Available Replication Groups** box.
3	Expand the tree in the **Available Replication Groups** box. **Result:** This displays the lower sub-groups.
4	Click on the group name in the **Available Replication Groups** list to select it. **Notes:** • To select multiple groups at table, module or application root level, press and hold the **Ctrl** key while selecting. • To select a block of groups, hold press and hold the **Shift** key while selecting.
5	Keeping the mouse depressed, drag the icon across to the **Allocated Replication Groups** list. Drop on the required node name by releasing the mouse button. **Result:** The replication group will be displayed under the selected node.
6	If a multiple selection is made, assign a common filter to the replication group on the Node Type Filter Selection screen.
7	Select the node type from the drop-down list. 
8	Click **OK**. **Result:** The replication group will be allocated to the selected node, if there are no dependencies on unselected replication groups.
9	If dependencies exist, the Missing Dependency screen will prompt you to add the dependant group.
10	Click **Yes**.  **Result:** The dependant replication group will also be added under the node.
11	Click **Save**. **Result:** The details will be saved to the database.

Adding the statistics replication group

Follow these steps to configure the statistics replication group.

Step	Action
1	In the **Table Replication** tab, **Available Replication Groups** box, under SMF_STATISTICS_DEFN, select the replication group for each application on the platform.
	Note: The SMF_STATISTICS_DEFN group contains all definitions.
2	Select the target node, for example SLC, for the application.
3	Click **Add** to allocate the group to the node name. **Result:** The statistics replication group will be configured for the application.
4	Repeat steps 1 through 3 for each application, if required.
5	Click **Save**.
6	Click **Create Config File**. **Result:** The Replication Confirmation prompt will appear indicating that the **replication.config** file has been created.
7	Click **OK**.

Changing primary status of an allocated group

Follow these steps to change the primary status of an allocated group:

Step	Action
1	In the **Table Replication** tab, expand the tree in the **Allocated Replication Groups** box. **Result:** This displays the lower sub-groups.
2	Click on the group name in the Allocated list. Keep the mouse button depressed.
	Notes: • To select multiple groups at table, module or application root level, press and hold the **Ctrl** key while selecting. • To select a block of groups, hold press and hold the **Shift** key while selecting.
3	Click the right mouse button. **Result:** A pop-up menu will appear.
4	Select **Set/Clear Primary**. **Result:** The primary flag will be associated to the allocated replication group. If the primary flag is already associated to the allocated replication group, it will be removed.
5	Click **Save**. **Result:** The details will be saved to the database.
6	Click **Create Config File**. **Result:** A Confirmation prompt will appear.
7	Click **OK**.
	Note: If there are problems with this replication then the system will display an error message. If this occurs, see *Service Management System Technical Guide*.

Delete an allocated group

Follow these steps to delete an allocated group.

Step	Action
1	In the **Table Replication** tab, expand the tree in the **Allocated Replication Groups** box. **Result:** This will display the lower sub-groups.
2	Click on the required group name in the Allocated list and right-click to view the menu options.
3	Click **Delete**. **Result:** The selected replication group will be removed from under the node.
4	If dependencies exist, the **Delete group dependency violation** warning will display a list of the dependent groups.
5	Select all listed dependencies and repeat steps 2 and 3. **Result:** The selected replication groups and their dependencies will be removed from under the node.
6	Click **Save**. **Result:** The details will be saved to the database.
7	Click **Create Config File**. **Result:** A Confirmation prompt will appear.
8	Click **OK**. **Note:** If there are problems with this replication then the system will display an error message. If this occurs, see *Service Management System Technical Guide*.

Important note - VWS

Do not delete allocated groups from the VWS. The VWS replication node is configured automatically when a billing engine is added on the CCS BE Configuration Screen. For more information, see *Charging Control Services User's Guide*.

Replication Node Types

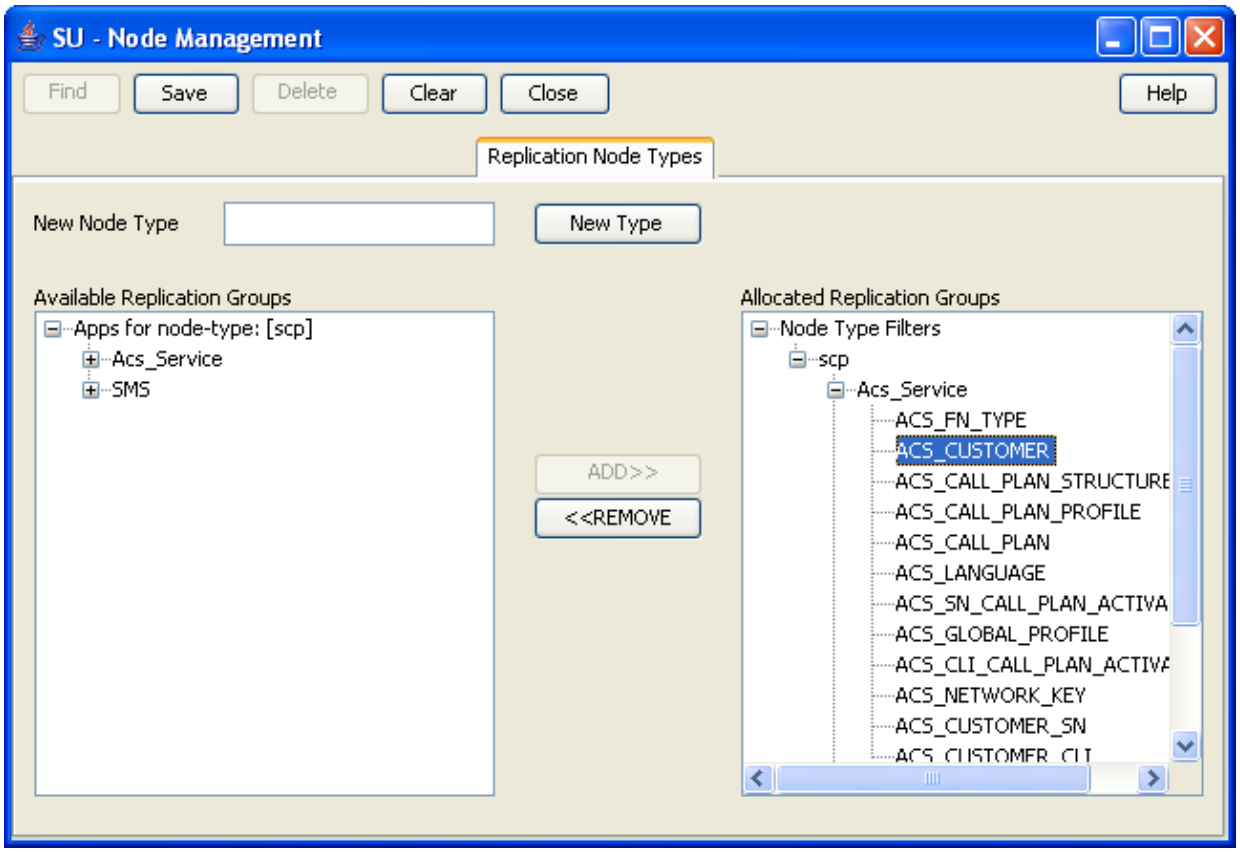
Introduction

The **Replication Node Types** tab of the Node Management screen is used for creating the filters through which multiple groups at table, module or application root level may be added to a node as a block on the **Table Replication** tab.

The **Replication Node Types** tab works in the same way as the **Table Replication** tab, except it also allows the addition of new node types. However, if the specified node type matches one that already exists in the system, then it cannot be added.

Replication Node Types tab

Here is an example of the **Replication Node Types** tab.



Replication Node Types fields

This table describes the function of each field.

Field	Description
Available Replication Groups	Displays a list of available groups for replication.
Allocated Replication Groups	Displays a list of available nodes for allocating the replication table groups.
New Node Type	Name of the node type filter which will be used for the adding block replication groups to a node.

Adding a node type

Follow these steps to add a new node type filter:

Step	Action
1	In the **Replication Node Types** tab, click **Clear**.
2	In the **New Node Type** field, enter the name of the new node type (required).

Step	Action
3	Click **New Type** to allocate the selected replication group to the required node name. **Result:** The replication group will be displayed under the selected node. **Note:** If the specified node type already exists, it cannot be added again.
4	Click **Save**. **Result:** The details will be saved to the database and the Save Complete message is displayed.
5	Click **OK**. **Note:** If there are problems with this replication then the system will display an error message. If this occurs, see *Service Management System Technical Guide*.

Deleting a node type

Follow these steps to delete a node type filter.

Step	Action
1	In the **Replication Node Types** tab, click **Clear**.
2	Expand the tree in the **Allocated Replication Groups** box to required node and right-click to view the menu options.
3	Click **Delete**. **Result:** The selected node type filter will be removed. **Note:** If dependent/children groups exist, the node type filter will not be deleted until the dependencies are deleted.

Allocating a replication group

Follow these steps to allocate a new replication group using the Replication Node Types tab.

Note: You can also use the *Table Replication* (on page 23) tab to allocate replication groups.

Step	Action
1	In the **Replication Node Types** tab, click **Clear**.
2	Expand the tree in the **Allocated Replication Groups** box to the required node name and select it. **Result:** The group list specific to the selected node will be displayed in the **Available Replication Groups** box.
3	Expand the tree in the **Available Replication Groups** box. **Result:** This displays the lower sub-groups.
4	Click on the group name in the **Available Replication Groups** list to select it. **Notes:** • To select multiple groups at table, module or application root level, press and hold the **Ctrl** key while selecting. • To select a block of groups, hold press and hold the **Shift** key while selecting.
5	Click **Add** to allocate the selected replication group to the required node name. **Result:** The replication group will be displayed under the selected node.

Step	Action
6	If a multiple selection is made, assign a common filter to the replication group on the Node Type Filter Selection screen.
7	**Choose Node Type** from the drop-down list.
8	Click **OK**. **Result:** The replication group will be allocated to the selected node, if there are no dependencies on unselected replication groups.
9	If dependencies exist, the Missing Dependency screen will prompt you to add the dependant group.
10	Click **Yes**. **Result:** The dependant replication group will also be added under the node.
11	Click **Save**. **Result:** The details will be saved to the database.

Removing an allocated group

Follow these steps to remove an allocated group using the **Replication Node Type** tab:

Step	Action
1	In the **Replication Node Type** tab, expand the tree in the **Allocated Replication Groups** box. **Result:** This displays the lower sub-groups.
2	Click on the group name in the list to select it. **Note:** To select multiple groups at table, module or application root level, press and hold the **Ctrl** key while selecting. To select a block of groups, hold press and hold the **Shift** key while selecting.
3	Click **Remove** to de-link the selected replication group from the node name. **Result:** The replication group will be removed from under the selected node, if there are no dependencies on unselected replication groups.
4	If dependencies exist, the Delete group dependency violation warning will display a list of the dependent groups.
5	Select all listed dependencies and repeat step 3. **Result:** The selected replication groups and their dependencies will be removed from under the node.
6	Click **Save**. **Result:** The details will be saved to the database. **Note:** If there are problems with this replication then the system will display an error message. If this occurs, see *Service Management System Technical Guide*.

Chapter 4

Configuring Users

Overview

Introduction

This chapter explains how to access and operate the User Management options.

User Management provides the ability to manage users and user permission templates.

In this chapter

This chapter contains the following topics.

User Management Module

Introduction

The User Management screen manages users and templates used in the SMS. It contains the following tabs:

- *User* (on page 34)
- *Template* (on page 45)
- *Template Creation* (on page 41)
- *Quality of Service* (on page 47)

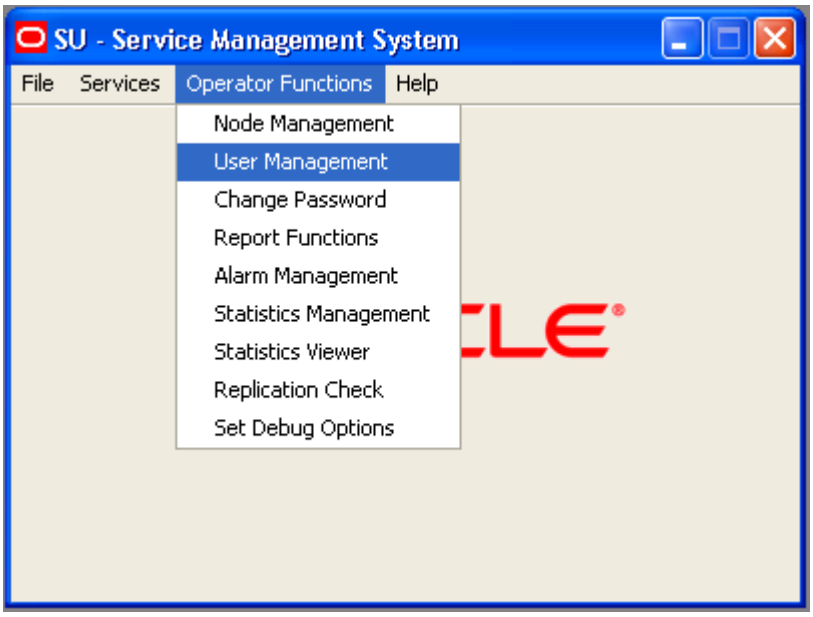
Users and templates

Each user's access to the SMS is defined by which templates they have been allocated. Each template specifies which parts of the SMS the user has access to, and what actions they can take in each part.

Accessing the User Management screen

Follow these steps to access the User Management screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action
	
2	Select **User Management**. **Result:** You see the User Management screen.

Users

Introduction

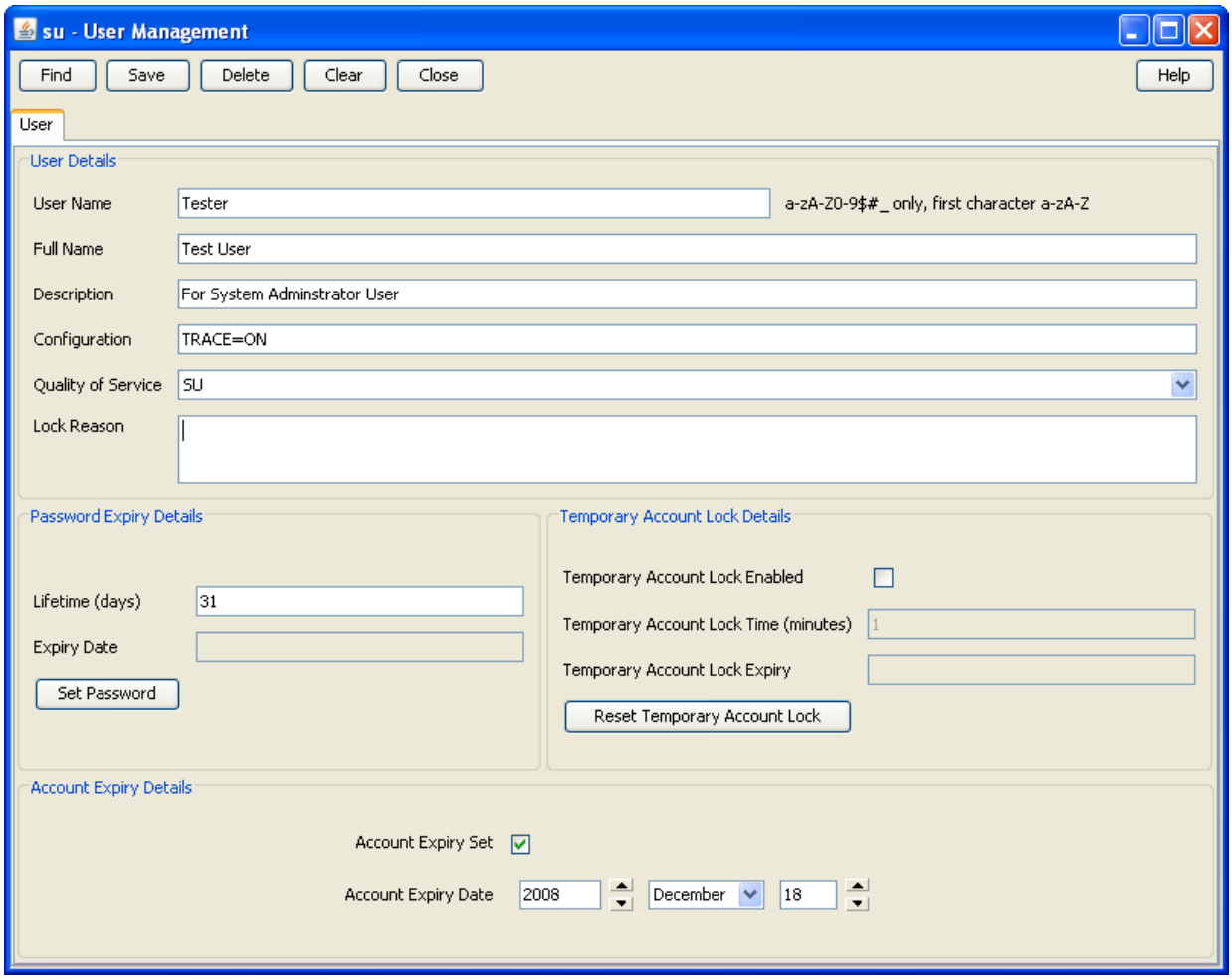
The **User** tab of the User Management screen enables you to create and maintain user accounts in the SMS.

When you create a new SMS user, the SMS assigns the Oracle profile defined in the defaultOracleProfile parameter in the **eserv.config** file to the new user. If the defaultOracleProfile parameter is not defined, the SMS assigns the standard Oracle profile to the new user by default. The Oracle profile includes the password verification function that determines the specific conditions for a valid password, such as the minimum length, number of digit characters, and so on. When you create or edit a user's password, the SMS verifies that you have entered an acceptable password by applying the verification function that is specified in the Oracle profile.

See *Service Management System Technical Guide* for more information about assigning Oracle profiles to new users.

User tab

Here is an example **User** tab.



User fields

This table describes the function of each field.

Field	Description
User Name	User name of the user. May be any combination of alphanumeric or special characters that produce a valid Oracle user name. This is the name Oracle assigns when adding new users; it cannot change. In the event that a user name must change, you must delete the account and add a new user with the correct name. This field is compulsory.
Full Name	Full name of this user. This is used is for identification of records in the find screens and for reporting purposes. This field is compulsory.

Field	Description
Description	Description of the user. This is used is for identification of records in the find screens and for reporting purposes. This field is optional.
Configuration	Configuration options for the user. These include Language, Tracing, or any other supported Java configuration. Multiple configuration options must be separated with a semicolon. **Format:** *option=value; option=value; ...* **Where:** *option* is configuration option. *value* is a supported parameter for that option. **Example:** LANGUAGE=ENGLISH For more information about the available configuration options, see *Valid configuration options* (on page 37).
Quality of Service	The Quality of Service drop down list enables you to specify the level of service this user will be provided. It is populated by the Quality of Service tab. For more information about configuring service levels, see *Quality of Service* (on page 47).
Lock Reason	Displays the reason that a user has been locked out of the database. This field is normally blank. If for any reason it is populated, the user will have no access to the system. This field may be populated by either the system or manually. If the **Temporary Account Lock Enabled** check box is not selected, the system will populate this field. If a user fails to log in to the system in three attempts, the system locks the account and the following text appears in the lock reason field: LOCKED: Failed login, maximum attempts exceeded. For more information about locked accounts, see *Locked users* (on page 38). **Warning:** When you create a user, leave this field blank to avoid creating a locked account.
Lifetime (days)	Number of days before user is required to change their password. This is used in combination with today's date to calculate the expiry date of the user's password. The expire date is calculated when a password is changed. If this field is left blank, the user's password will never expire.
Expiry Date	Date when a user's password expires. After this date has expired, the user will not be allowed access to the database. This field will be automatically populated when the password lifetime is set and the password is changed. **Formula:** SYSTEM DATE + Password Lifetime = Password Expiry Date
Temporary Account Lock Enabled	If this check box is selected, after too many consecutive failed attempts to login, the system will set a time-based-lock. If this check box is not selected, after too many failed attempts to login the system will save data to the Lock Reason field.

Field	Description
Temporary Account Lock Time (minutes)	Minutes the system will add to the system date to calculate when a time-based-lock expires. Will accept either any value between 1 and 1440 (1 day). If no value is supplied, the time-based-lock will remain active until deactivated by the Reset Temporary Time Lock button.
Temporary Account Lock Expiry	If a time-based-lock has been triggered for this user, this field displays the date and time when the lock will expire. **Note:** This field is cleared when one of the following occurs: • The account's password is successfully changed • The user logs in successfully after the lock expiry date has been passed
Account Expiry Set	If this check box is selected, the account will expire at the time specified in the Account Expiry Date fields. **Note:** If this box is selected, but the Account Expiry Date fields do not specify a date, the account will never expire.
Account Expiry Date	If the Account Expiry Set check box is selected, these fields set the time the account will expire. If the current date is later than the date set in these fields, the account will be locked. **Note:** When you set these fields, the date they specify must be between 1 day and 1 year in the future.

Valid configuration options

Configuration Option	Description
TRACE	Can be set to 'TRUE', 'ON' or '1'. This turns tracing on in the java console. Default is off.
LANGUAGE	Can be set to any valid language, but *value* must exist as a file in the following directory: **/IN/html/sms/language directory/***value***.lang** If this field is empty, the default language for the system will be used. For more information about setting up additional languages, see *Service Management System Technical Guide*.

Adding users

Follow these steps to add a new user account.

Step	Action
1	If the fields on the **User** tab are populated with user data, click **Clear**. **Result:** The data in the fields will be removed.
2	In the **User Name** field, enter the user's username as it will appear in the system.
3	In the **Full Name** field, enter the user's full name.
4	In the **Description** field, enter a description for the user.
5	In the **Configuration** field, enter the language for the user.

Step	Action
6	In the **Quality of Service** field, select the appropriate service level for the user from the drop down list.
7	In the **Password Details** section, enter the number of days for expiry of the password in the **Lifetime** field or enter a specific expiry date in the **Expiry Date** field.
	Note: Setting the number of days until expiration or expiry date configures the user's Oracle database profile password expiration interval. The default profile expiration interval of UNLIMITED (for Oracle 10g databases) or 180 days (for Oracle 11g databases) is used if no value is specified for the new user here. See the Oracle Database Security Guide for the version of Oracle database you are using for a detailed description of how to use password management and protection.
8	Click **Set Password**. **Result:** You see the Set SMS User Password screen.
9	Enter and confirm the user's temporary password and click **OK**. See *Setting the User Password* (on page 40).
10	If you want to set up a time-based-lock on the account, select the **Temporary Account Lock Enabled** check box, and enter the number of minutes a triggered lock will remain active for in the **Temporary Account Lock Time (minutes)** field.
11	If you want to set an expiry date for this account, select the **Account Expiry Set** check box and set the date the account will expire in the **Account Expiry Date** fields.
12	Click **Save**. **Result:** A User Details confirmation prompt is displayed.
13	Click **OK**.

Changing a user

Follow these steps to change a user's account details.

Step	Action
1	Find the required user on the **User** tab. See *Using the Find Screens* (on page 12).
2	Change the user's details as required.
3	Click **Save**.

Deleting users

Follow these steps to delete an existing user account.

Step	Action
1	Find the required user on the **User** tab. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The Delete Confirmation prompt will appear.
3	Click **OK**. **Result:** The user account will be deleted from the database.

Locked users

Users can be locked out by three methods:

1 When a system administrator saves any data in the Lock Reason field on the **User** tab

2 By using an invalid user name and password combination three times in a row

3 When their account has expired

If a user is locked out due to invalid login attempts:

- An entry is added to the SMF_AUDIT table in the SMF database recording the users, terminals and times of invalid login attempts
- One of the following occurs:
  - The system saves data to the Lock Reason for the user
  - If time-based-locking is enabled, a time-based-lock is triggered for the user

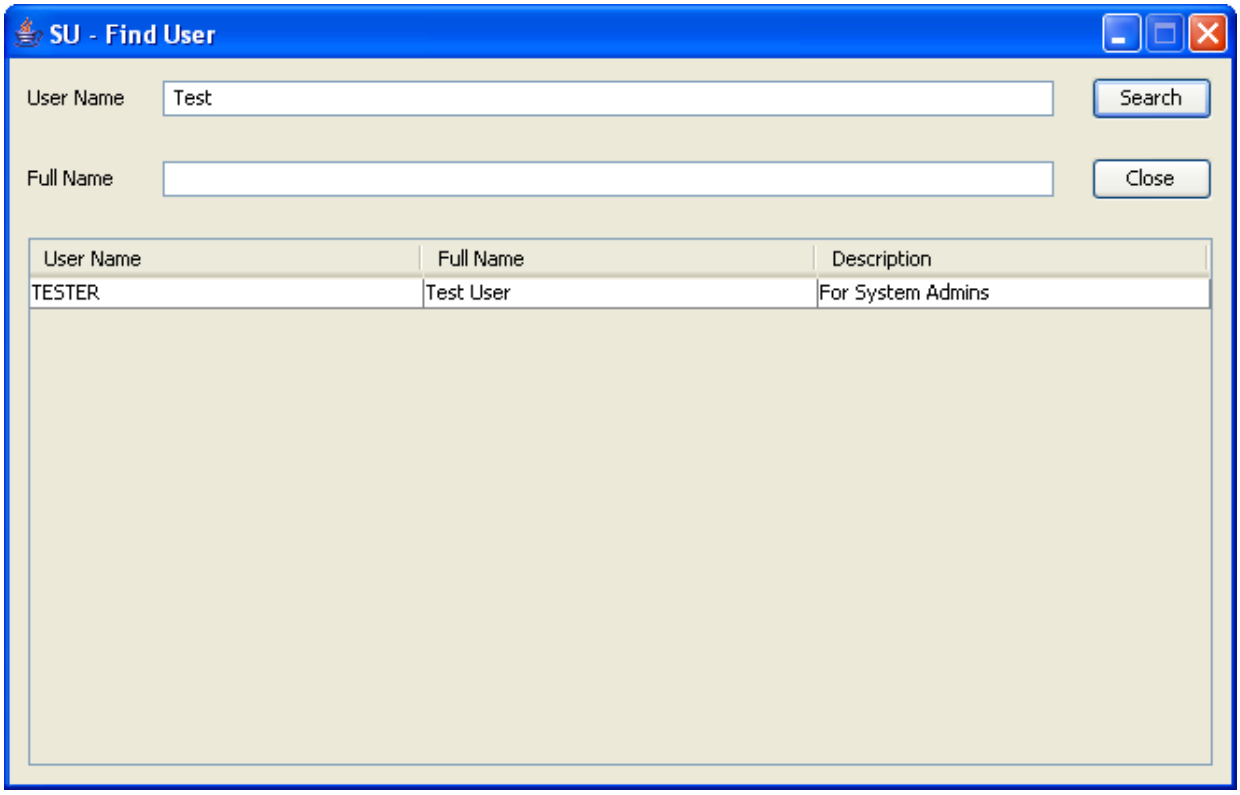
Unlocking a locked user

Follow these steps to unlock the user's account:

Step	Action
1	Find the required user on the **User** tab. See *Using the Find Screens* (on page 12).
2	If there is data in the **Lock Reason** field, delete it.Find the required user on the **User** tab. See *Using the Find Screens* (on page 12).
3	If the Temporary Account Lock Expiry field is showing an expiry date for a time-based-trigger, click **Reset Temporary Account Lock**.
4	If the account has expired, set the Account Expiry Date fields to a date in the future.
5	Click **Save** to save the changes.
6	Reset the user's password. For instructions about resetting passwords, see Creating a password.

Find User screen

Here is the **User Find** screen.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Setting the User Password

Introduction

This screen enables you to create a user's temporary password. The following screen appears when creating a user's password for the first time.

The user will be prompted to change the password after successfully logging onto the system for the first time.

Password fields

The table below describes the function of each field.

Field	Description
New Password	User password. For security purposes, it is advisable to enter a password of at least 6 to 8 characters in length.
Confirmation	Confirmed password.

Creating a password

Follow these steps to create a new temporary user password.

Step	Action
1	On the **User** tab of the User Management screen, click **Set Password**. **Result:** The Set SMS User Password screen will appear. 
2	In the **New Password** field, enter the password. **Note:** An error message displays if you enter an invalid password.
3	In the **Confirmation** field, re-enter the password to confirm it.
4	Click **OK**. **Result:** The new password will be set.

Creating User Templates

Introduction

When assigned to a user, a user template specifies what parts (screens and tabs) the user is able to access. Each part has access permissions.

Access permissions may be one or more of the following types:

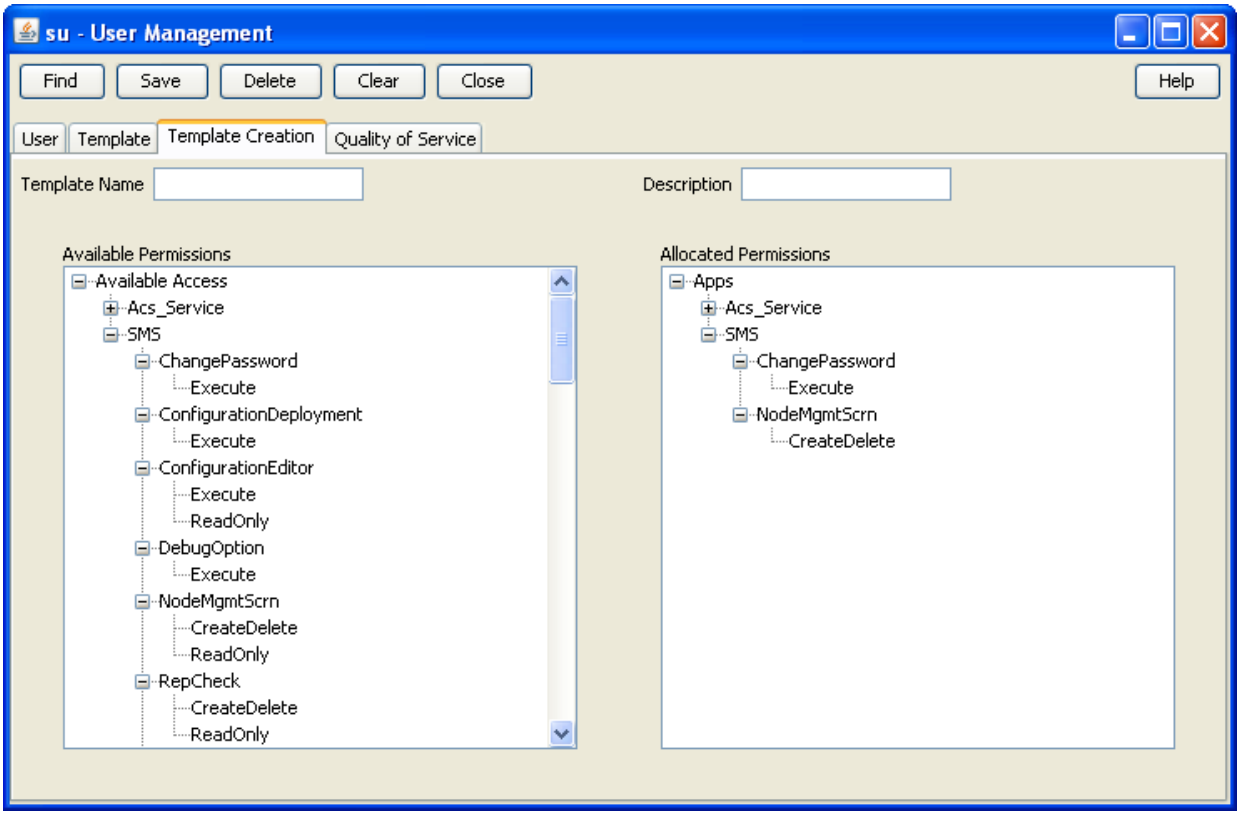
- Read
- Modify
- Create
- Delete
- Access
- Execute

If a part is not allocated to a user's template, the functionality provided by the part will not be available to the user.

The **Template Creation** tab on the User Management screen allows you to create, modify, and delete user templates.

Template Creation tab

Here is an example **Template Creation** tab.



Template Creation fields

The following table describes the function of each field on the **Template Creation** tab.

Field	Description
Template Name	The name of the template. • The name must be unique. • The **Template Name** field is compulsory.
Description	A description of the template. • A description is required is for identification of records in the find screens and for reporting purposes. • The **Description** field is compulsory.
Available Permissions	A list of parts and associated permissions available to the template. • You can expand or contract the list. ▪ To expand or contract individual parts, click the + or - symbol. ▪ To expand or contract the whole list, right-click anywhere in the **Available Permissions** field. From the menu, select the required option. The options are:

Field	Description
	- Expand All - Expand to First Level - Collapse All • The create, delete, modify and read permissions are arranged in a hierarchy where a permission at one level also includes permissions for levels below it. The order of permissions, with 1 being the highest, is: 1. CreateDelete 2. ReadModify 3. ReadOnly For example, if you choose CreateDelete, you also receive permission to modify and read. • The access and execute permissions are not part of the create, delete, modify and read hierarchy. • You can assign only one permission level for any part.
Allocated Permissions	A list of parts and associated permissions allocated to the template. You can expand or contract the list and delete parts from it. • To expand or contract individual parts, click the + or - symbol. • To expand or contract the whole list, right-click anywhere in the **Allocated Permissions** field. From the menu, pick the option you require. The options are: ▪ Delete Selection ▪ Expand All ▪ Expand to First Level ▪ Collapse All • To delete a part, see *Removing a permission from a template* (on page 44).

Creating a template

Follow these steps to create a user template.

Step	Action
1	If any of the **Template Name**, **Description** or **Allocated Permissions** fields contain information, click **Clear**.
2	Type a unique name in the **Template Name** field.
3	Type a description of the template in the **Description** field.
4	In the **Available Permissions** field, expand the branch of the list you are interested in: click the + symbol adjacent to the branch name. **Result:** The contents of the **Available Permissions** list expands to show all parts and permissions for the branch selected.
5	Search the branch for the part you want to assign to the template. Move the mouse pointer over the required permission. Hold down the left mouse button and drag the permission into the **Allocated Permissions** field. **Result:** The selected part and permission appears in the **Allocated Permissions** field. **Note:** Multiple selections are allowed by holding down **Ctrl** when selecting.
6	After you have added all the permissions you require, click **Save**. **Result:** The new user template is saved to the database.

Changing a user template

Follow these steps to change a user template.

Step	Action
1	If necessary, locate and open the template: click the **Find** button. See *Using the Find Screens* (on page 12).
2	To add a new permission, follow steps 4 and 5 of the previous procedure.
3	To change a permission: **1** Search the list in the **Available Permissions** field for the part to change. **2** Move the mouse pointer over the new permission. **3** Hold down the left mouse button and drag the permission into the **Allocated Permissions** field. **Result:** In the **Allocated Permissions** field, the permission for the selected part changes.
4	Click **Save**. **Result:** The changed user template is saved to the database.

Removing a permission from a template

Follow these steps to remove a permission from a user template.

Step	Action
1	If necessary, locate and open the template: click the **Find** button. See *Using the Find Screens* (on page 12).
2	In the **Allocated Permissions** field, move the mouse pointer over the permission you want to remove, left-click and then right-click. **Result:** The right-click menu appears.
3	Pick **Delete Selection** from the menu. **Result:** The selected part and permission disappears from the **Allocated Permissions** field.
4	Click **Save**. **Result:** The selected part and permission is removed from the user template.

Deleting a user template

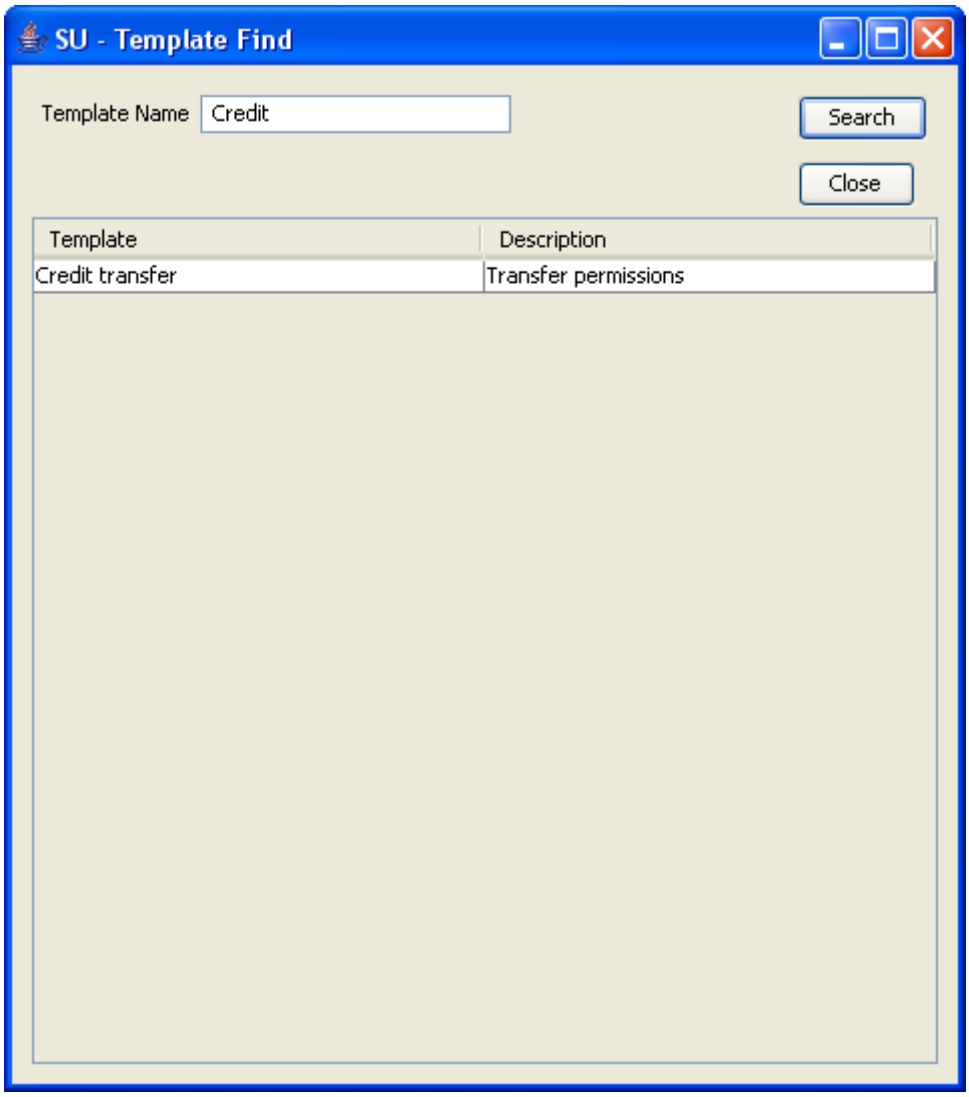
Follow these steps to delete a user template.

Note: You cannot delete a template that is currently defining a user's access.

Step	Action
1	If necessary, locate and open the template and click the **Find** button. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The Deleting confirmation prompt appears.
3	Click **OK**. **Result:** The template is deleted from the database.

Template Find screen for User Management

Here is an example of the Template Find screen when the **Template Creation** tab is active.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

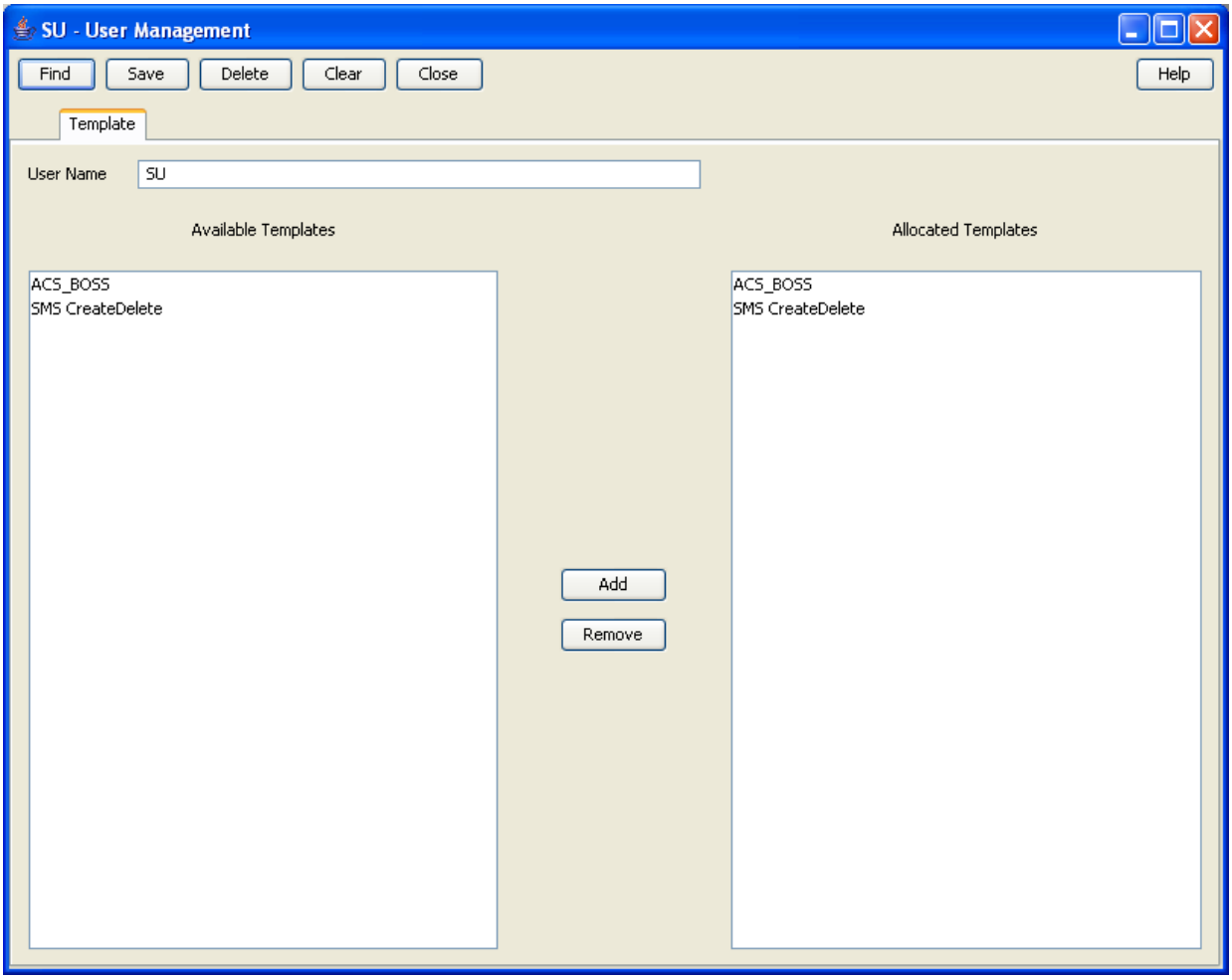
Assigning Templates

Introduction

The **Template** tab of the User Management screen enables you to allocate existing templates to a user. The user will have whatever permissions are specified in the templates they are allocated.

Template tab

Here is an example **Template** tab.



Template fields

The table below describes the function of each field.

Field	Description
User Name	Name of the user whose template allocation is currently being defined.
Available Templates	List of all templates available on the system.
Allocated Templates	List of templates allocated to a user. A user may only access those parts of the SMS and associated services which are defined in the templates in the Allocated Templates list. In addition to giving access to the various parts, templates also give various levels of access (that is, Read only, Read/Modify, and Create).

Assigning a template to a user

Follow the steps below to assign a template to a user.

Step	Action
1	Find the required user on the **Template** tab. See *Using the Find Screens* (on page 12). **Result:** The User to assign a template to will appear in the User Name field.
2	In the **Available Templates** list, select the template to assign to the user.
3	Click **Add**. **Result:** The template will appear in the Allocated Templates list.
4	Click **Save**. **Result:** The details will be saved to the database.

Removing a template allocation

Follow these steps to remove a template from a user.

Step	Action
1	Find the required user on the **Template** tab. See *Using the Find Screens* (on page 12).
2	Click on the required template in the **Allocated Templates** list.
3	Click **Remove**. **Result:** The template will be removed for the Allocated Templates list.
4	Click **Save**. **Result:** The changes will be saved to the database.

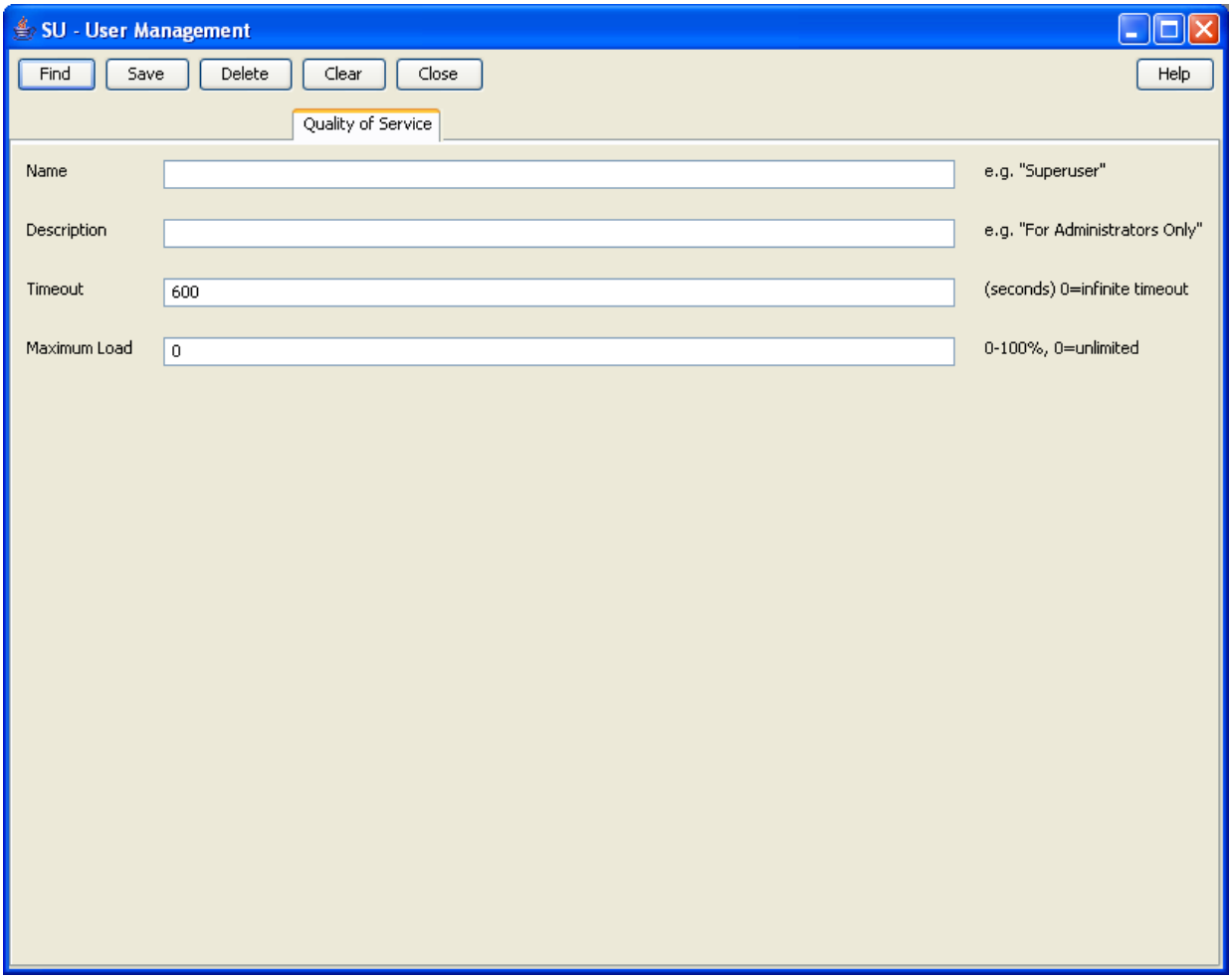
Quality of Service

Introduction

The **Quality of Service** tab of the User Management screen enables you to add, edit or delete a Quality of Service record. Quality of Service records enable you to provide different levels of service to different users.

Quality of Service tab

Here is an example **Quality of Service** tab.



Quality of Service fields

The table below describes the function of each field.

Field	Description
Name	Name of this quality of service record.
Description	Description of this quality of service record.
Timeout	Maximum number of seconds inactivity before a user's database connection is closed. **Allowed values:** • 0 • 300 through 999999 If set to 0, the connection will never be terminated.

Field	Description
Maximum Load	The maximum percentage of non-reserved database connections used before a user with this quality of service cannot log in. **Example:** If 50% of the non-reserved connections are in use: • A user with maximum load set to 30% will not be able to log in (and will be presented with a message stating that they have insufficient priority to log in), but • A user with maximum load set to over 50% will be able to successfully log in. **Allowed values:** • 0 • 1 though 100 If this value is set to 0, users with this quality of service will always be able to log in. **Notes:** The system reserves: • A number of connections for Oracle and the SMS system processes • A connection for each user whose quality of service has maximum load set to 0 Any remaining connections are available for users whose quality of service maximum load is in the range 1-100. Oracle will impose a limit as specified in the processes parameter in the **initSMF.ora** file in **$ORACLE_HOME/dbs** directory on the SMS.

Automatic reconnect

The connection will be re-created when the user subsequently uses the system in such a way as to need a database connection.

Note: If the user's maximum load parameter indicates a new connection from them would be denied, their reconnection will fail.

Adding Quality of Services

Follow these steps to add a new quality of service definition.

Step	Action
1	In the User Management screen, select the **Quality of Service** tab.
2	If the fields are populated with data, click **Clear**.
3	In the **Name** field, enter the name of this quality of service definition.
	Note: If the name is the same as an existing record, this process will update the existing record instead of creating a new record.
4	In the **Description** field, type a description of this quality of service definition.
5	In the **Timeout** field, enter the number of seconds a user can be inactive before their connection to the database is closed.
6	In the **Maximum Load** field, enter the CPU load percentage above which the user's connection to the database will be closed.

Step	Action
7	Click **Save**. **Results:** • The details will be saved to the database • The Save Quality Of Service prompt will appear to confirm that the record has been saved.
8	Click **OK**.

Edit a Quality of Service

Follow the steps below to modify an existing quality of service record.

Step	Action
1	Find the quality of service to change. See *Using the Find Screens* (on page 12).
2	Change the quality of service fields as required.
3	Click **Save**.

Deleting a Quality of Service

Follow these steps to remove an existing quality of service record.

Step	Action
1	Find the required quality of service. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** If the user: • Has permission to delete a quality of service and the quality of service is not currently in use, the Deleting Quality of Service prompt will appear. Go to step 3. • Does not have permission to delete a quality of service and/or the quality of service is in use, a dialog box will be displayed indicating that the action is not allowed.
3	Click **OK**. **Result:** The quality of service record will be deleted from the database.

Chapter 5

Changing Passwords

Overview

Introduction

This chapter explains the change password function. This function enables non-Super User users to change their password.

In this chapter

This chapter contains the following topics.

Change Password Module

Introduction

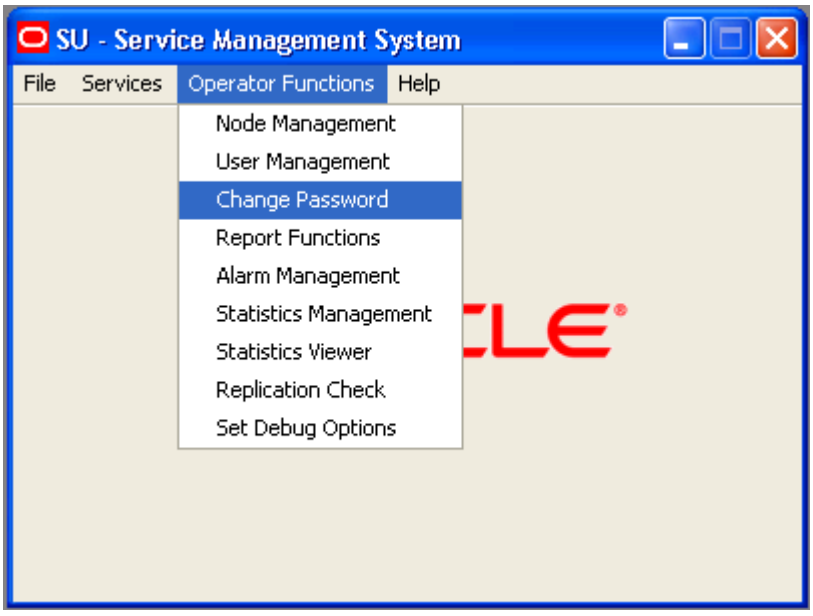
The Change Password module enables ordinary users to change the password for their SMS user account.

Accessing the Change Password screen

Follow these steps to access the Change Password screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



2 Select **Change Password**.

Result: You see the Change Password screen.

Note: The Change Password option on the Operator Functions menu appears only if a template associated with the user has been allocated the Execute ChangePassword permission.

Password Verification Function

Password verification functions are a feature in the Oracle database and allow a site to configure their own, usually stricter, password verification policy. A password policy is site dependent, based on the password verification function specified.

A verification function is installed in the SYS schema in the Oracle database, which is then associated with a user profile in the database. The profile can be allocated to one or more users. When users attempt to change their password in either the **Change Password** or **User Management** tabs in the **Operator Functions** feature, and their password is not compliant with the password policy, they receive the following dialogue:

The password does not change but instead the user must specify a new password that is compliant with the password policy.

Password Policy

A password policy allows a site to specify that a password meets a number of requirements. For example the requirements could include one or more of the following requirements:

- Contains a minimum number of characters
- Contains a minimum number of digits
- Contains a minimum number of letters
- Contains a minimum number of special characters
- Does not contain double-quote characters
- Differs from a previous password by a specified number of characters

Example Password Policy

The following is an example of a password policy:

- Contains a minimum of 9 characters
- Contains a minimum of 2 digits
- Contains a minimum of 2 letters
- Contains a minimum of 2 special characters
- Differs from a previous password by 3 characters

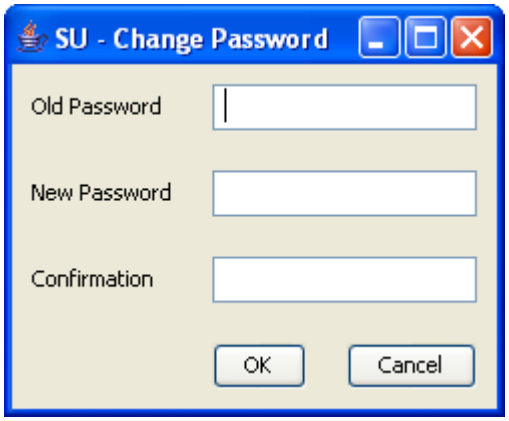
Change Password

Introduction

The Change Password screen enables ordinary users to change the password for their SMS user account.

Change Password Screen

Here is an example Change Password screen.



Field descriptions

The table below describes the function of each field.

Field	Description
Old Password	Current user password.
New Password	New password. For security reasons, a password must be at least 8 characters long.
Confirmation	Confirmed password.

Changing a password

Follow these steps to change your password.

Note: Password rules must be adhered to.

Step	Action
1	Enter your current password in the **Old Password** field.
2	Enter your new password in the **New Password** field. **Note:** An explicit error message is displayed when an invalid password is entered.
3	Re-enter your new password in the **Confirmation** field.
4	Click **OK** to save the changed password.

Chapter 6

Maintaining Alarms

Overview

Introduction

This chapter explains how to access the Alarm Management screen and describes the screen contents. Alarm Management screens inform users of alarms that have occurred in the system as they happen. If the system detects any unexpected behavior, the alarm screens help the user locate the problem.

It is strongly recommended that Alarm Management screens be monitored regularly.

To make the alarm monitoring system more useful, you can use the **Alarm Control** tab to modify the severity of a particular alarm or alarm type.

In this chapter

This chapter contains the following topics.

Alarm Management Module

Introduction

Use the **Alarm Management** module to configure and perform alarm management functions.

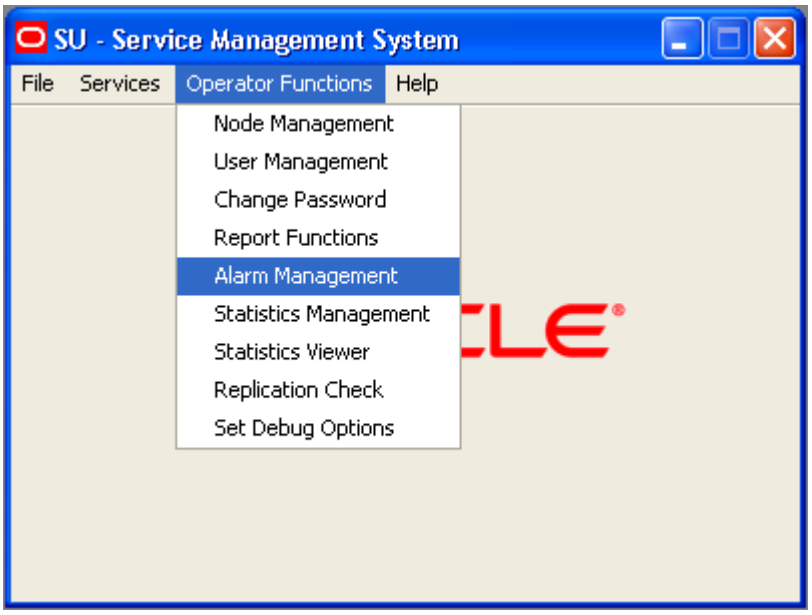
It enables you to perform the following tasks:

- View alarms
- Handle alarms
- Configure the forwarding of alarms
- Configure automatic alarm escalation
- Configure alarm classification and presentation

Accessing the Alarm Management screen

Follow these steps to access the Alarm Management screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action
	
2	Select **Alarm Management**. **Result:** You see the Alarm Management screen.

Managing Alarms

Introduction

The **Alarm** tab of the Alarm Management screen enables you to monitor and handle alarms. The list of alarms is refreshed automatically. A filter may be specified to select the alarms to be displayed.

Alarm overview

Alarms are messages collected from nodes running Oracle applications, including the SMS. They indicate the status of and actual and potential faults in these nodes.

Upon receipt, alarms are first matched to an alarm definition (see *Alarm Definitions* (on page 83) for details). Alarms that match an alarm definition are treated in accordance with the matching definition; unmatched alarms are treated differently. Unless the alarm definition requires otherwise, the alarms are then passed to the Alarm Management system.

When the Alarm Management system receives notification of an alarm, it checks to see whether the alarm has occurred before. If it was the:

- *First* occurrence of that alarm then it performs three functions:
  - Adds a color-coded line to the Alarm table. The color corresponds to the severity of the alarm (see *Alarm fields* (on page 58))
  - Brightens the corresponding Alarm button
  - Adds 1 to the first number in the alarm count of the corresponding Alarm button
- *Second or more* occurrence of that alarm then it performs two functions:
  - Adds to the alarm count on the corresponding color-coded line in the Alarm table. The alarm count appears in the Count column (see *Alarm fields* (on page 58)).
  - Adds 1 to the second number in the alarm count of the corresponding Alarm button

The important thing to remember about alarms is that they:

- Repeat until the problem is rectified (unless they are information only, in which case they are part of normal functioning and will continue)
- Correspond to a particular platform and program

Example of repeating alarms

Machine A on the network generates an error alarm. The problem was not rectified, so it generates another error alarm of the same type.

Machine B then generates an error alarm caused by the same type of problem.

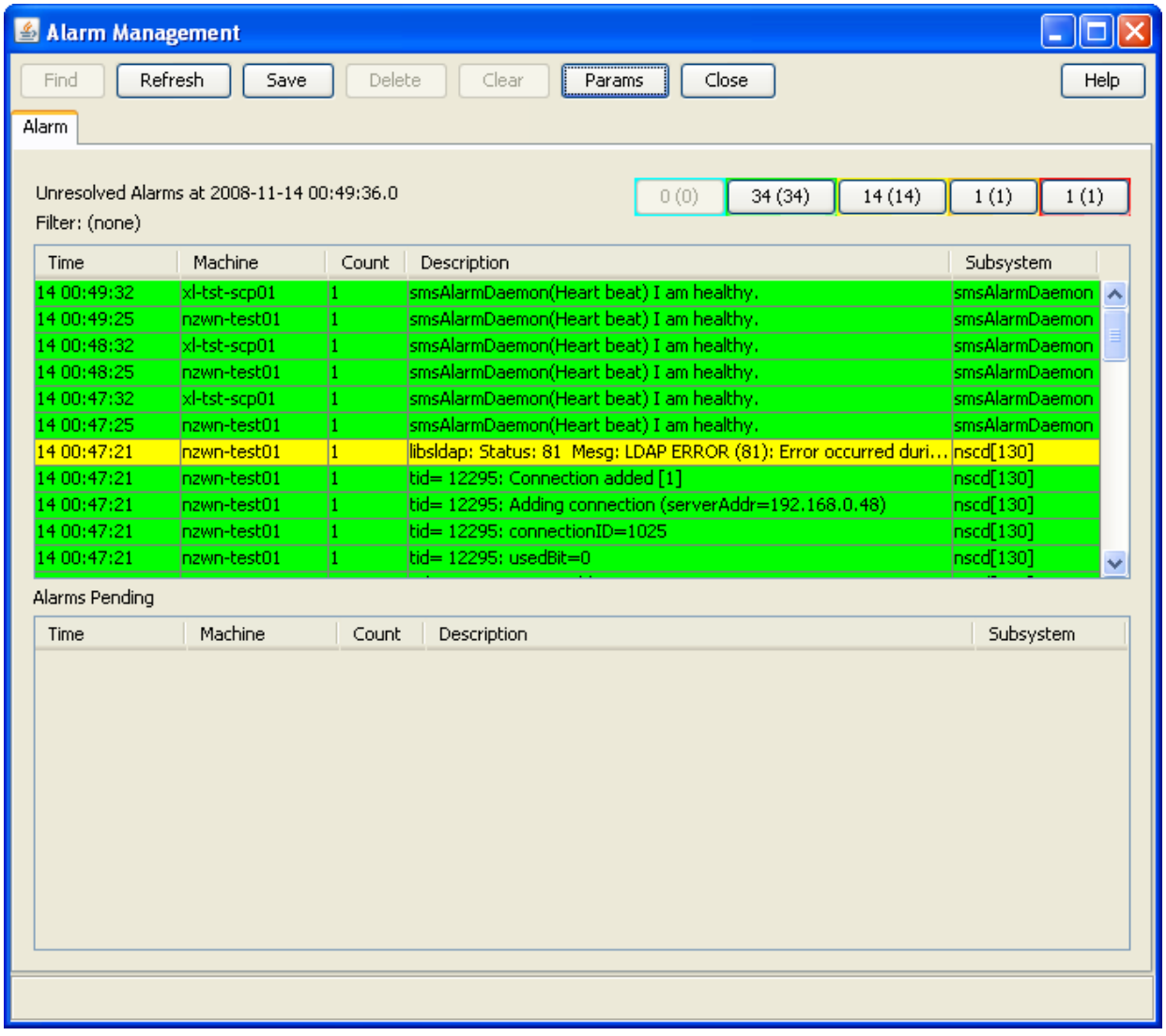
Therefore, the Alarm Management system will show two orange lines in the Alarm grid; one from Machine A and one from Machine B.

Machine A line will show a count of 2, Machine B line will show a count of 1.

The Alarm button is highlighted with the numbers 2(3) appearing.

Alarm tab

Here is an example **Alarm** tab displaying instances of alarms that have occurred in the system.



Alarm tab buttons

This table describes the function of each button.

<table>
<tr><th>Button</th><th>Description</th></tr>
<tr><td>Severity buttons</td><td>These buttons provide a summary view of alarms that match the button activated. There are five levels of severity for alarms.
The different colors on the buttons represent levels of severity. These are:
<table>
<tr><th>Button</th><th>Description</th></tr>
<tr><td>Blue</td><td>Clearance of previous alarm</td></tr>
<tr><td>Green</td><td>Information Only</td></tr>
<tr><td>Yellow</td><td>Warning</td></tr>
<tr><td>Orange</td><td>Error</td></tr>
<tr><td>Red</td><td>Critical</td></tr>
</table>
When an alarm is:
• Activated, the button is highlighted
• Rectified, the button is dimmed</td></tr>
<tr><td>Refresh</td><td>The data will be reread from the database.</td></tr>
<tr><td>Params</td><td>Opens the associated settings screen to change the parameter setting for the screen. From the:
• Alarm tab it opens the Alarm Settings screen
• Alarm Definition tab it opens the Alarm Definition Settings screen.</td></tr>
</table>

Alarm fields

This table describes the function of each field.

Field	Description
Unresolved Alarms Table	
	This table displays alarms that have not been resolved. The alarm status is unresolved.
Time	Time the alarm was generated. **Note:** This is the system time (that is, SMF database time), not necessarily the user's local time.
Machine	Platform name. Where the alarm was generated.

Field	Description
Count	Alarm count. Number of times the alarm has occurred. The period of time for which multiple instances of the same alarm will be shown as a count is configured for `smsAlarmDaemon`. For more information about setting the time period for the `smsAlarmDaemon`, see *Service Management System Technical Guide*.
Description	Alarm description. Displays a description of the alarm that was generated.
Subsystem	Subsystem that generated the alarm.
Alarm Type ID	The unique identifier for this type of alarm.
Event Type	The Event Type is attached to alarm instances by the alarm definition and may be changed as required. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Probable Cause	The probable cause field displays the TMN standard probable causes. It is congruent with the association between event type and probable cause specified in the TMN recommendations (see ITU-T M.3100).
Severity	The severity of the alarm.
Specific Problem	The specific identification of the fault.
Recommended Action	Describes what action is recommended to resolve all instances of this type of alarm.
Additional text	Any additional text or information about this type of alarm will be displayed in this column.
Autoclear Period	The autoclear period determines how long (in minutes) an alarm will be available in the **Alarm** tab, before it is automatically cleared by smsAlarmManager. For more information about smsAlarmManager, see *Service Management System Technical Guide*.
Notes	Any Notes about this type of alarm will be displayed in this column.
Alarms Pending Table	
	This table displays the alarms that have been modified but not closed.

Note: The columns that are visible in the tables may be changed by the user using the Visible Columns screen. See *Changing the screen display* (on page 71) for details.

Selecting an alarm

Alarms may need to be selected for many reasons, including those listed below:

- Change the alarm severity
- Place the alarm in the pending list
- Resolve an alarm
- Add a comment to the alarm

Follow these steps to select individual alarms:

Method One:

To jump to the next alarm from a particular severity, click the Severity button of the level you wish to view.
Result: The system will highlight the next available alarm of that severity or higher in the table.

Method Two:

Double-click on the required alarm in the Alarm table.

Selecting multiple alarms

Follow these steps to select multiple alarms.

Method One:

This method selects individual alarms, out of sequence.

Step	Action
1	Press and hold **Ctrl**.
2	Click on each alarm required. **Result:** The system highlights the alarm to show that it is selected.

Method Two:

This method selects a range of alarms.

Step	Action
1	Press and hold **Shift**.
2	Click on the start of the range and then the last entry in the range. **Result:** All entries within the range are selected.

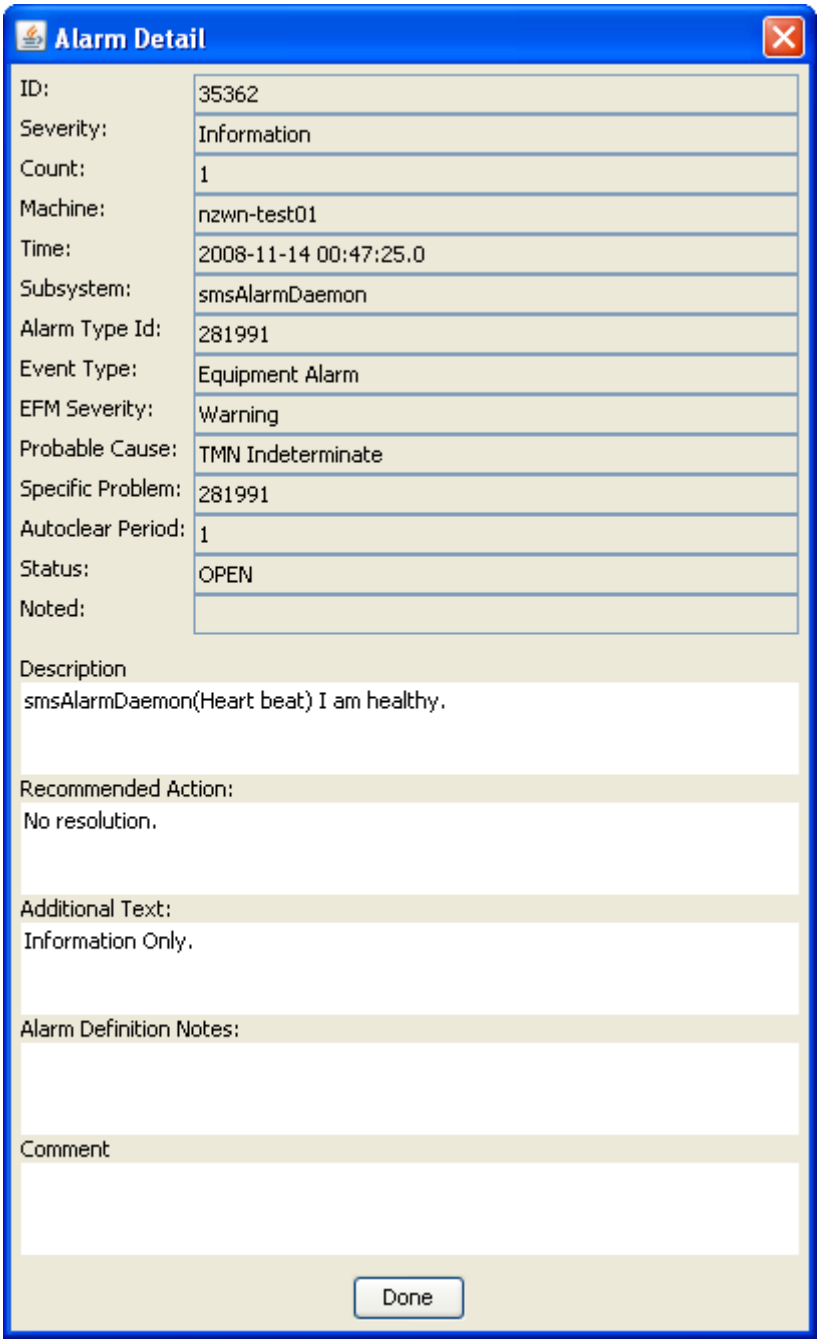
Changing alarm comments

Follow these steps to amend the comment field in the alarm.

Method One

Step	Action
1	Select the required alarm in the Alarm table. **Result:** The Alarm Detail screen displays.

Step	Action



2	In the **Comment** field, enter any required comment.
3	Click **Done.**
	Result: The alarm moves from the Unresolved Alarms table to the Alarms Pending table.

Method Two

Step	Action
1	Highlight the required alarm in the Alarm table.
2	Right-click the mouse button.
	Result: You see a menu including the following options:

Step	Action
	• Annotate: Problem is being fixed • Annotate: Known recurring problem • Annotate: Known temporary problem
3	Select the appropriate Annotate option. **Result:** The text selected appears in the **Comment** field of the alarm, and the alarm moves from the Unresolved Alarms table to the Alarms Pending table.

Alarm Detail screen fields

This table describes the function of each field.

Field	Description
ID	The unique identifier for this alarm instance.
Severity	The severity which which this alarm instance was raised by the system. **Note:** This is the Oracle Severity not the x733 Severity.
Count	The number of instances that this type of alarm has been raised by the system in the period set by the display period field in the setting screen.
Machine	The name of the platform on which this alarm instance was raised.
Time	The time (taken from the platform on which the alarm instance was raised) at which the alarm occurred.
Subsystem	The subsystem that raised the instance of the alarm.
Alarm Type Id	The identifier of the type of alarm that this instance is an occurrence of.
Event Type	The event type; which will be one of: • communicationsAlarm • qualityOfServiceAlarm • processingErrorAlarm • equipmentAlarm • environmentAlarm. The Event Type is attached to alarm instances by the alarm type definition. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Probable Cause	Shows the TMN standard probable causes. It is congruent with the association between event type and probable cause specified in the TMN recommendations (see ITU-T M.3100) The probable cause is attached to alarm instances by the alarm type definition. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Specific Problem	Shows the specific identification of the fault. The specific problem is attached to alarm instances by the alarm type definition. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Autoclear Period	This displays how long (in minutes) an alarm will be available in the **Alarm** tab, before it is automatically cleared. This is attached to the alarm instance by the alarm type definition.

Field	Description
Status	Shows the status of the alarm, this will be one of; open, pending, closed. Alarms that have an open status will be displayed in the Unresolved Alarms table of the **Alarm** tab and alarms with a pending status will be displayed in the Alarms Pending table of the **Alarm** tab.
Noted	This field shows when the alarm was last commented or closed.
Description	This is the text of the alarm that is raised by the system. This may not be changed.
Recommended Action	Describes what action is recommended to resolve all instances of this type of alarm. The recommended action is attached to alarm instances by the alarm type definition.
Additional Text	Any additional text or information about this type of alarm will be shown in this field. The additional text is attached to alarm instances by the alarm type definition.
Alarm Definition Notes	Any user added notes about this type of alarm will be displayed in this field. The notes text is attached to alarm instances by the alarm type definition.
Comment	This field is used to add any comments required to this instance of the alarm.

Changing alarm severity

Follow these steps to change the severity of an alarm.

Step	Action
1	Highlight the required alarm in the Alarm table using any method described previously.
2	Right-click the mouse button. **Result:** You see a menu, including the following options: • Change severity to: Information • Change severity to: Warning • Change severity to: Error • Change severity to: Critical
3	Select the appropriate Change severity option. **Result:** The color of the alarm changes to the new corresponding level, and the total alarm counts is updated. **Note:** This is the Oracle Severity not the x733 Severity.

Closing an alarm

Follow these steps to close an alarm.

Step	Action
1	Highlight the required alarm in the Alarm table using any method described previously.
2	Right-click the mouse button. **Result:** You see a menu, including the following options: • Fault closed • Fault reopened
3	Select the **Fault closed** option. **Result:** The alarm is removed from the Unresolved Alarms table.

Changing closed alarms

Follow these steps to view, change, or reopen a closed alarm.

Step	Action
1	Click **Params**. **Result:** You see the Alarm Settings screen.
2	From the **Alarm State** drop down list, select **Closed**.
3	Click **Done**. **Result:** The Alarm Management screen displays the closed alarms.
4	Highlight the required alarm in the Alarm table using any method described previously.
5	Right-click the mouse button. **Result:** You see a menu, including the following options: • Fault closed • Fault reopened
6	Select the option as required/ described previously to change the alarm.
7	Select the **Fault reopened** option as required to reactivate the alarm. **Result:** The alarm is removed from the Resolved Alarms table.

Alarm Settings

Introduction

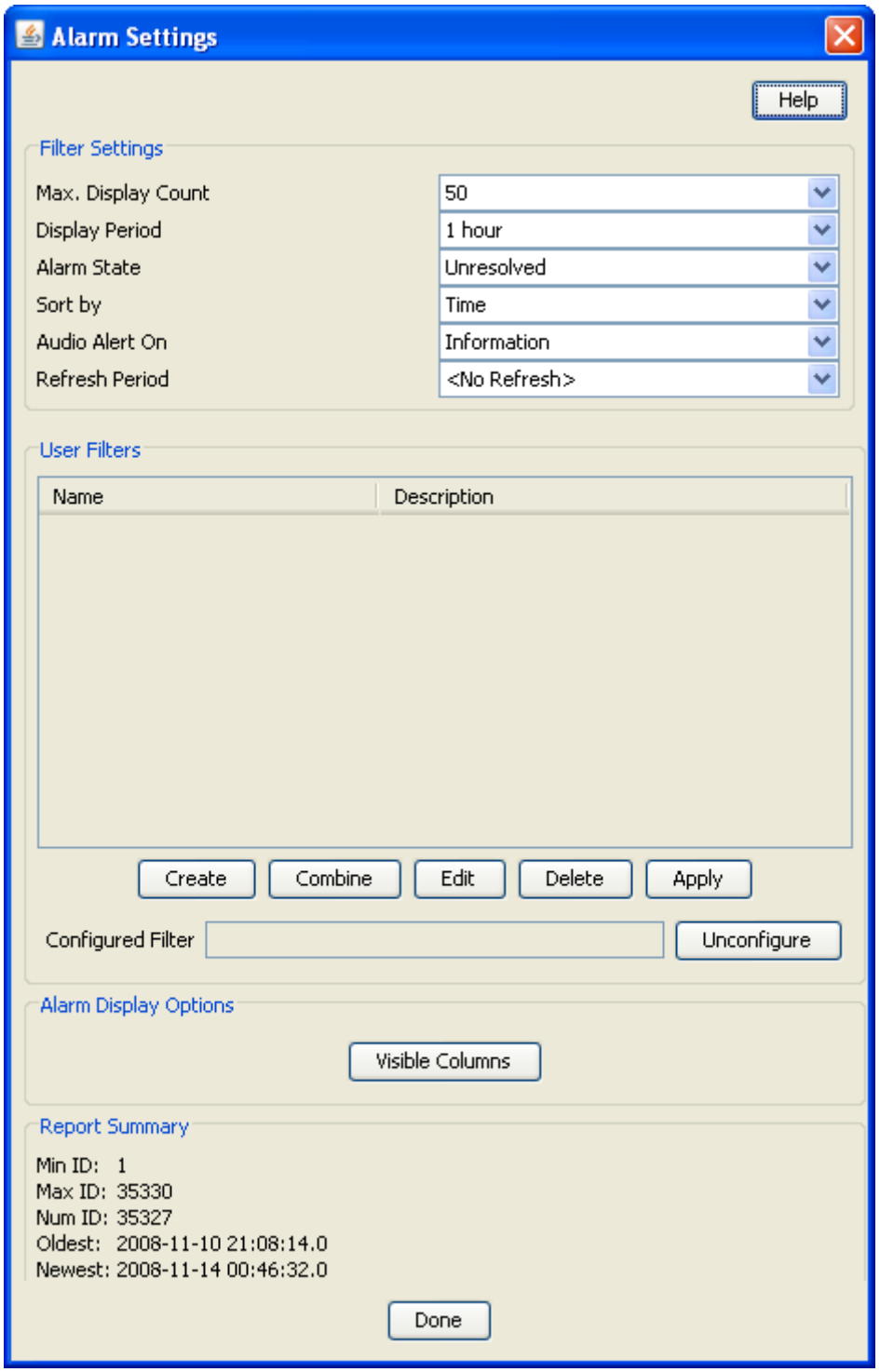
Use the Alarm Settings screen to define the type of alarm you wish to see in the alarm grids on the **Alarm** tab. It acts as a filter, excluding alarms that you may not wish to view.

Accessing the Alarms Settings screen

To access this screen, click **Params** in the upper right corner of the Alarm Management screen when the **Alarm** tab is displayed.

Alarm Settings screen

Here is an example Alarms Settings screen.



Changing alarm display settings

Follow these steps to change the settings that control the alarms and what detail from those alarms is displayed on the **Alarms** tab.

Step	Action
1	In the Alarm Management screen, click **Params**. **Result:** You see the Alarm Settings screen.
2	Make changes to the field settings, as required. For more information about the settings you can use, see *Alarm Settings field areas* (on page 66).
3	Click **Done**. **Result:** The details are saved to the database.

Alarm Settings field areas

The Alarm Settings screen has several distinct parts to it, each of which control different aspects of the alarm display. These parts are:

Field	Description
Filter Settings	These settings determine the alarms that are retrieved from the database for display in the alarms screen. For more information about this section, see *Filter Settings fields* (on page 66).
User Filters	Filters enable you to select alarm types that are to be displayed. These allow different types of alarms to be hidden from view. This area displays the name and description of the filters which are available. For more information about: • Filters, see *Creating a standard filter* (on page 67). The only filter which is being applied to the **Alarms** tab is the filter in the **Configured Filter** field. • Applying filters, see *Applying filters* (on page 70)
Alarm Display Options	Enables you to determine which columns of information that you want to see, and the ordering of these columns. For more information about displaying columns, see *Visible Columns* (on page 71).
Report Summary	A report on the alarms that are in the system. The data displayed in this section gives a summary on all the alarms that are in the system.

Note: The Filter Setting, User Filters, and Alarm Display Option settings are maintained separately for each SMS user.

Filter Settings fields

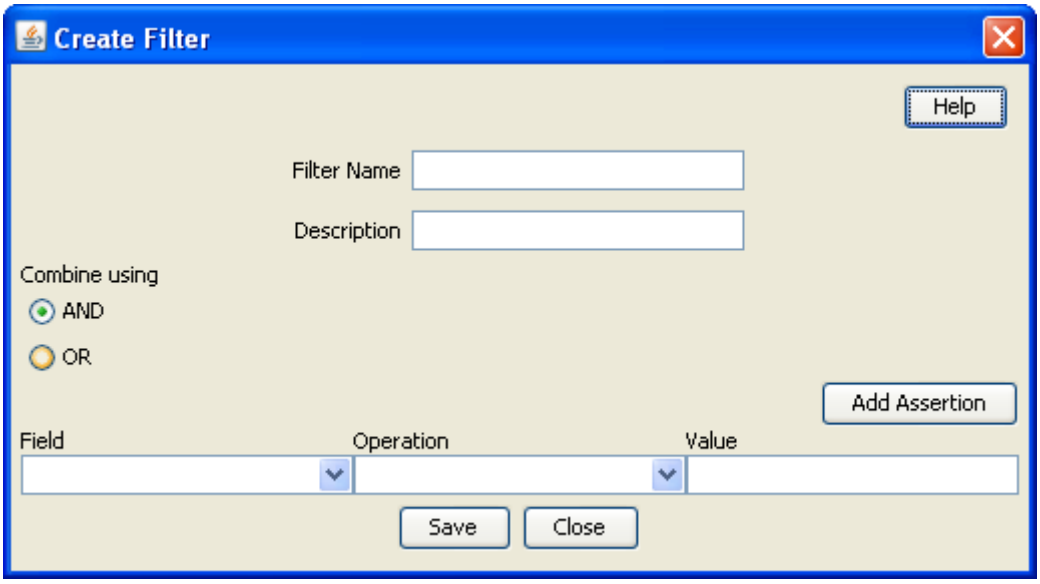
This table describes the function of each field in the Filter Settings section of the Alarm Setting screen.

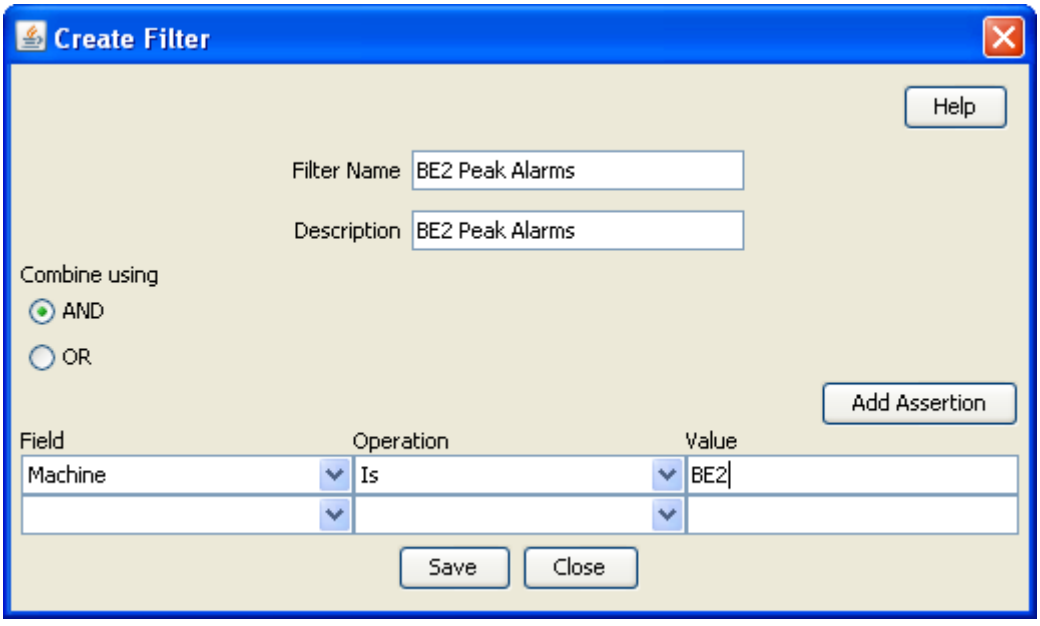
Field	Description
Max Display Count	The maximum number of alarms to be retained in the scroll back buffer from the pull down list. The entries in this list are 50, 100, 200 and 300. **Note:** This sets the maximum number of entries to display on the screen. There may be more than the maximum found that match the filters, but only the first 50 (100, 200, 300) are displayed.
Display Period	Period of time that alarms are displayed.
Alarm State	Determines the alarms to display in the unresolved panel. You can display alarms that are either: • Unresolved • Closed
Sort By	How the alarms are sorted in the display list.
Audio Alert on	Severity level to produce audible sound. Anything below this severity does not produce a sound. Anything at or above this level produce, a sound. **Example:** If you select `Error`, the only alarms that produce a warning sound are either "Error" or “Critical”.
Refresh Period	How often the Alarms screen automatically refreshes with new information. **Note:** If none is chosen, you can still refresh the list of alarms by clicking **Refresh**.

Creating a standard filter

Follow these steps to create a standard filter to display only alarms that match the filter criteria.

Note: You can create more complex filters by combining filters into combination filters using the Combine function. For more information, see *Combining filters* (on page 70).

Step	Action
1	On the Alarm Settings screen, click **Create**. **Result:** The Create Filter screen appears. 
2	In the **Filter Name** field, enter a unique name for the filter. **Note:** This name may be up to 20 characters in length.
3	If appropriate, enter a description for the filter in the **Description** field. This field is optional.
4	Select the combination method which will apply to the assertions defined at the bottom of the screen. For a single assertion filter the combination method selected is not relevant, but for multiple assertion filters the combination method determines how the assertions are related. **Tip:** All assertions in the filter are combined using the selected value. A combination of 'AND' assertions and 'OR' assertions cannot be created in a single filter. This may be achieved using combinations of filters.
5	From the **Field** drop down list, select the field that alarms are to be filtered on. The drop down list displays all the options that may be filtered against.

Step	Action
6	Select the operation that is required. The operations that are supported are below: • Is • Is not • Before • After • Contains • Doesn't contain • Begins with • Ends with • Greater than • Less than **Note:** The operations that are available are different depending on the field that is selected. Only valid operations for each field are displayed.
7	Enter the value that the selected field is to be matched against. **Note:** This field is either a text field or a drop-down list, depending on the field that was selected.
8	To create a multiple assertion filter, click **Add Assertion**. **Result:** Another assertion line is added below the first. 
9	Repeat steps 5 through 8 to add the assertions for this filter. **Note:** A maximum of ten assertions are allowed per filter.
10	Click **Save**. **Result:** The changes to the filter are saved.
11	Click **Close** to close the screen. **Result:** The Create Filter screen closes and the filter is added to the User Filters table.

Note: The filters created using this screen may then be used in the Combining Filters screen to create more complex filters than is possible using this screen alone.

User Filters buttons

This table describes the function of each button.

Button	Description
Create	Use this button to create a new filter. **Result:** The Create Filter screen appears. For details on using this screen, see *Creating a standard filter* (on page 67).
Combine	Use this button to create a new filter by combining two existing filters. **Result:** The Combine Filters screen appears. For details on using this screen, see *Combining filters* (on page 70).
Edit	Use this button to edit the selected filter. **Note:** This button will open either the Combine Filters screen or the Create Filter screen according to the way the filter was created.
Delete	Use this button to delete the selected filter.
Apply	Use this button to apply the selected filter to the alarms. **Result:** Only the alarms that match the applied filter will be displayed in the alarms table on the **Alarms** tab of the Alarm Management screen. **Note:** You can only apply one filter to the alarms display at any one time. To apply more than one filter, use the Combine function, and apply the combined filter.
Unconfigure	Use this button to unconfigure the filter which is currently applied. This stops the current filter from applying. **Note:** The filter which is currently applied is displayed in the Configured Filter field next to this button.

User Filters fields

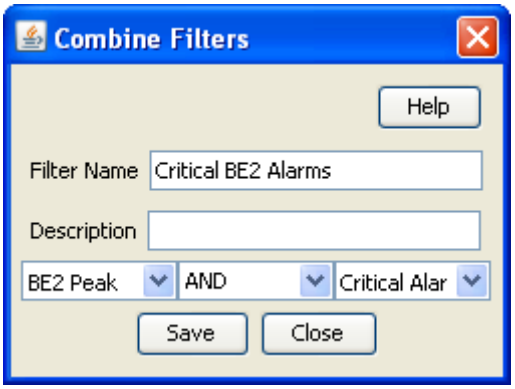
This table describes the function of each field.

Field	Description
Name	Name given to the filter
Description	Textual description of the filter
Configured Filter	This field displays the name of the filter that is current being applied to the alarm display.

Combining filters

Follow these steps to combine several simple filters and create a more complex filter.

Step	Action
1	Click **Combine**. **Result:** The Combine Filters screen will open.

Step	Action
	
2	In the **Filter Name** field, enter a name for the filter. **Note:** This name may be up to 20 characters in length and must be unique for the user.
3	If appropriate, enter a description for the filter in the **Description** field. This field is optional.
4	From the drop down list to the left of the screen, select the first filter use in this combined filter.
5	From the drop down list in the middle of the screen, select the operation that is to be used when combining the two filters.
6	From the drop down list to the right of the screen, select the second filter to use in this combined filter.
7	Click **Save**. **Result:** The changes to the filter are saved.
8	Click **Close** to exit from the screen. **Result:** The combined filter is added to the User Filters list.

Example

If a filter in the form '(A and B) and not C' is required it could be done in the following way.

1. Create three basic filters A, B and C.
2. Combine filters A and B using the combine functionality to create filter X.
3. Combine the new combination filter X with filter C using the 'AND NOT' operation.

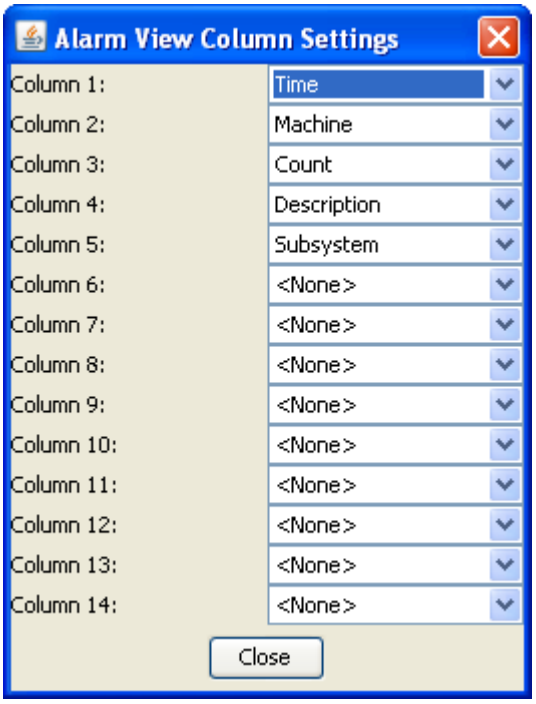
Applying filters

Follow these steps to apply filters to the Alarms to see only the required alarms.

Step	Action
1	On the **Alarms** tab, click **Params**. **Result:** The Alarm Settings screen appears.
2	In the User Filters section, select the filter to apply to the alarms displayed on the **Alarms** tab.
3	Click **Apply**. **Result:** The loaded filter will be applied to the alarm display, and only alarms that match that filter will be displayed.

Visible Columns

Follow these steps to change the screen display on the **Alarm** tab.

Step	Action
1	To change the screen display, click **Visible Columns**. **Result:** The Alarm View Column Setting screen opens. 
2	For each column, select the data that is to be displayed. This allows you to set the columns that are to be viewed and the order in which they are to be displayed.
3	Click **Close**.

Columns that may be displayed

This table describes the function of each column that can be displayed on the **Alarm** tab.

Field	Description
Time	Time the alarm was generated. **Note:** This is the system time (that is, SMF database time), not necessarily the user's local time
Machine	Platform name. Where the alarm was generated.
Count	Alarm count. Number of times the alarm has occurred. The period of time for which multiple instances of the same alarm will be shown as a count is configured for smsAlarmDaemon. For more information about setting the time period for the smsAlarmDaemon, see *Service Management System Technical Guide*.
Description	Alarm description. Displays a description of the alarm that was generated.

Field	Description
Subsystem	Subsystem that generated the alarm.
Alarm Type ID	The unique identifier for this type of alarm.
Event Type	The Event Type is attached to alarm instances by the alarm definition and may be changed as required. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Probable Cause	The probable cause field displays the TMN standard probable causes. It is congruent with the association between event type and probable cause specified in the TMN recommendations (see ITU-T M.3100)
Severity	The Oracle severity of the alarm, not the x733 Severity.
Specific Problem	The specific identification of the fault.
Recommended Action	Describes what action is recommended to resolve all instances of this type of alarm.
Additional text	Any additional text or information about this type of alarm will be displayed in this column.
Autoclear Period	The autoclear period determines how long (in minutes) an alarm will be available in the **Alarm** tab, before it is automatically cleared by smsAlarmManager
Notes	Any notes about this type of alarm will be displayed in this column.

Configuring Alarm Notifications

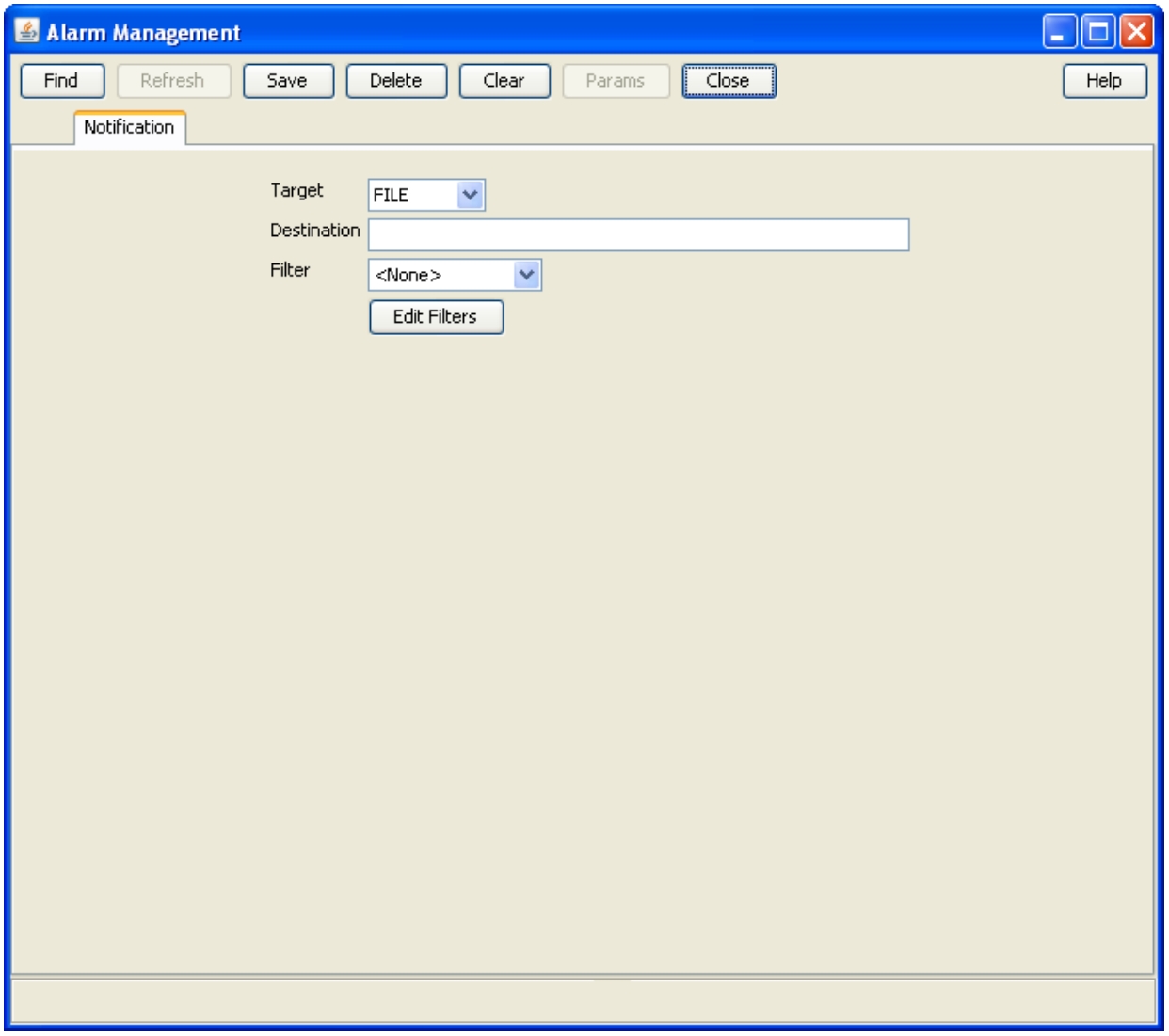
Introduction

The **Notification** tab enables you to create notification streams of alarms. Each stream is defined by its type, or target, its destination (which is target specific) and a filter, which selects the alarms to be forwarded to the destination.

There may be any number of streams and each alarm may be forwarded to multiple destinations. Note that the processing overhead of forwarding alarms depends on the number of Alarm Notifications and on the complexity of their filters.

Notification tab

Here is an example **Notification** tab.



Notification fields

This table describes the function of each field.

Field	Description
Target	Target for the notification. The targets include: • File • Q3 • NFM • SNMP • NORELAY
Destination	Destination address of the target. This table lists which destination information to enter for each target type.

Field	Description	
	If the target is...	**then the destination is...**
	a file	the file name, including the file path if required.
	Q3	the host name or IP address of the Q3 target.
	SNMP	the host name or IP address of the SNMP target.
	NFM	the host name or IP address of the NFM target.
	NORELAY	not required.
Filter	Alarms matching this filter will be forwarded to the target.	
Edit Filters	This button opens the Alarm Relay Filters screen to allow filters to be edited.	

Adding a notification

Follow these steps to add a new notification.

Step	Action
1	If the fields on the **Notification** tab are populated with data, click **Clear**.
2	From the **Target** drop down box, select the notification point the alarm will be sent to.
3	In the **Destination** field, enter the details required for the target set in step 2.
4	Select the filter that is to be used to determine which alarms are sent out. Having no filter selected will relay all alarms.
5	Click **Save**. **Result:** The details will be saved to the database.

Changing a notification

Follow these steps to change the notification:

Step	Action
1	Find the required notification on the **Notification** tab. See *Using the Find Screens* (on page 12).
2	Change the notification details as required.
3	Click **Save**. **Result:** The changes will be saved to the database.

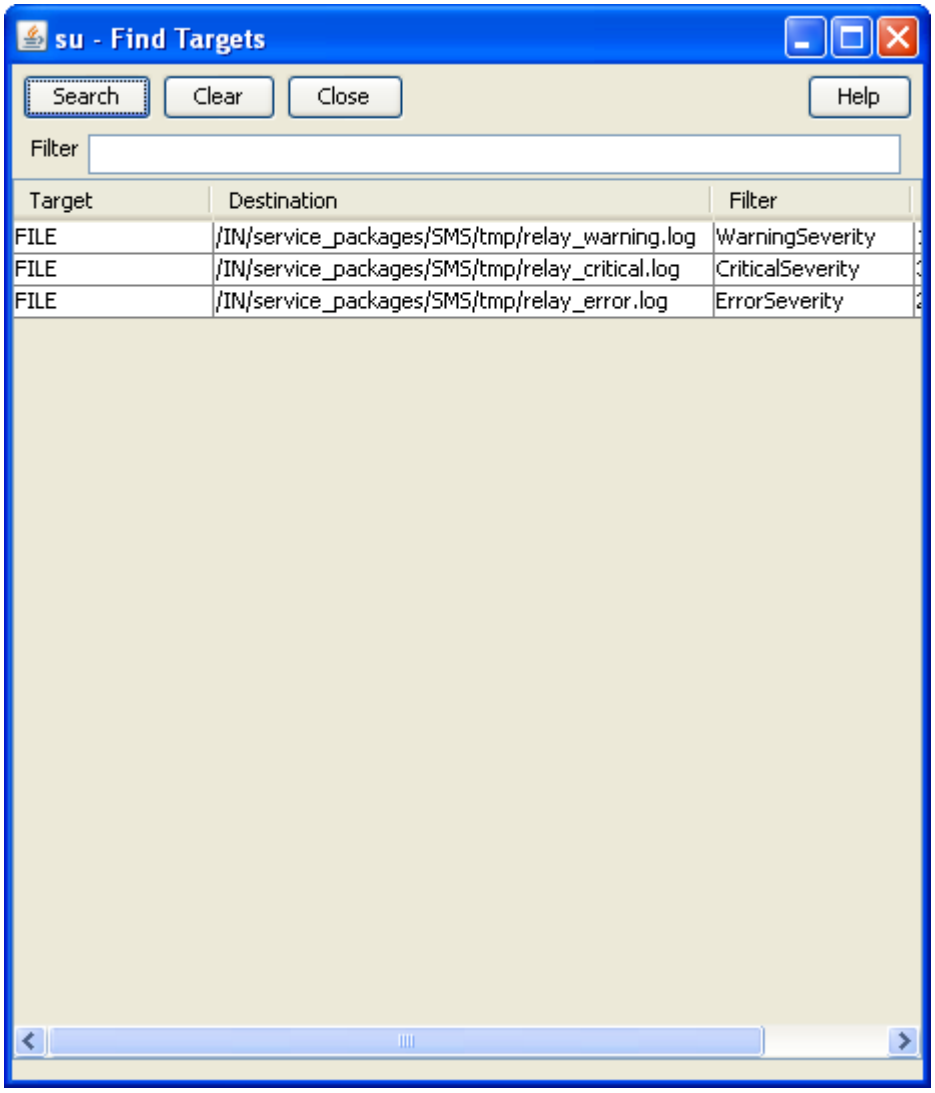
Deleting a notification

Follow these steps to remove a notification.

Step	Action
1	Find the required notification on the **Notification** tab. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The alarm will be deleted from the database.

Find Targets screen

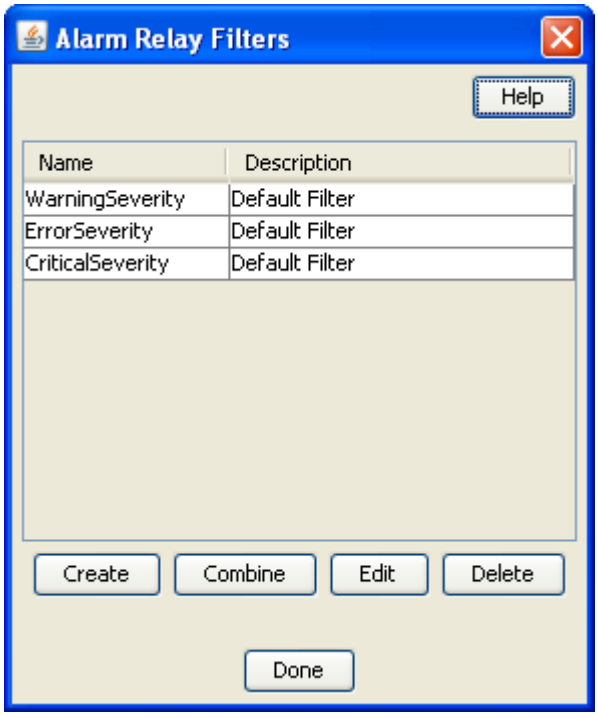
Here is an example of the **Find Targets** screen, which is used to find alarm notification rules.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Find Targets screen

Here is the **Alarm Relay Filters** screen, which is used to filter alarms to ensure that only the required alarms are sent.



Note: This screen is accessed through the **Edit Filters** button on the alarm **Notification** tab.

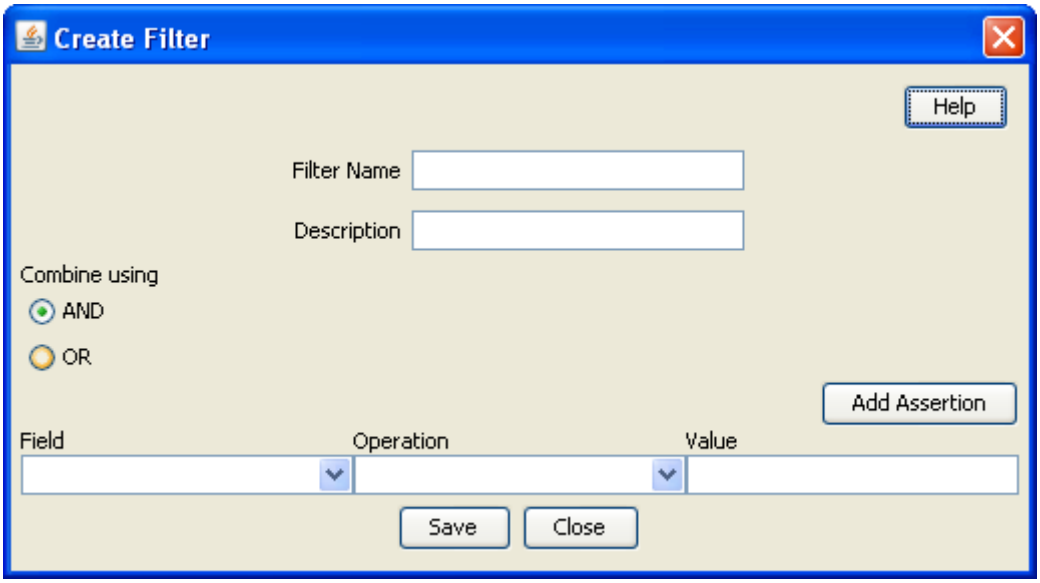
Alarm Relay Filters fields

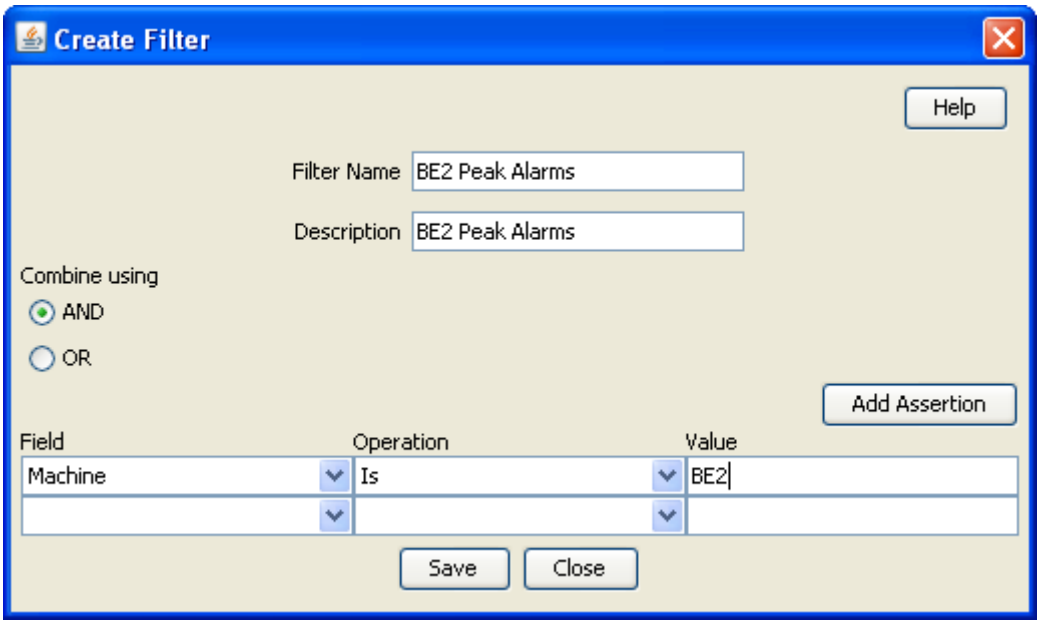
This table describes the function of each field.

Field	Description
Name	Name given to the filter
Description	Textual description of the filter
Create	Use this button to create a new filter. **Result:** The Create Filter screen appears. See *Creating a standard filter* (on page 67) for details on the use of this screen.
Combine	Use this button to create a new filter by combining two existing filters. **Result:** The Combine Filters screen appears. See *Combining filters* (on page 70) for details on how to use this screen.
Edit	Use this button to edit the selected filter. **Note:** This button will open either the Combine Filters screen or the Create Filter screen according to the way the filter was created.
Delete	Use this button to delete the selected filter.

Creating a filter

Follow these steps to create a filter to display only alarms that match the filter criteria.

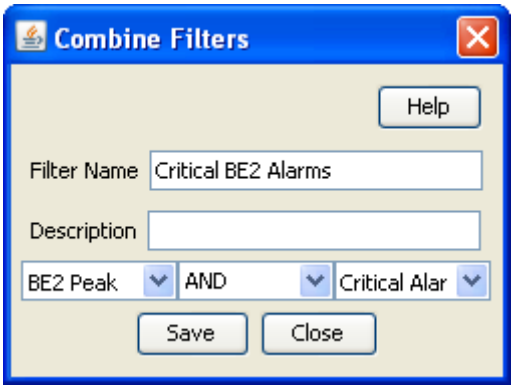
Step	Action
1	On the Alarm Relay Filters screen, click **Create**. **Result:** The Create Filter screen appears. 
2	Enter a name for the filter. **Note:** This name may be up to 20 characters in length and must be unique for the user.
3	If required, enter a description for the filter. This is optional.
4	Select the combine value that is required. For a single assertion filter the combine value selected is not relevant, but for multiple assertion filters the combine selection determines how the assertions are related. **Note:** All assertions in the filter are combined using the selected value. A combination of 'and' assertions and 'or' assertions cannot be created in a single filter. This may be achieved using combinations of filters.
5	Select the **Field** that alarms are to be filtered on. The drop down list displays all the options that may be filtered against.
6	Select the operation that is required. The operations that are supported are below: • Is • Is not • Contains • Doesn't contain • Begins with • Ends with • Greater than • Less than **Note:** The operations that are available differ depending on the field that is selected. Only valid operations for each field are displayed.
7	Enter the value that the selected field is to be matched against.

Step	Action
8	To create a multiple assertion filter, click **Add Assertion**. **Result:** Another assertion line is added below the first.  **Note:** A maximum of ten assertions are allowed per filter.
9	Repeat steps 5 through 8 as required.
10	Click **Save**
11	Click **Close** to close the screen

Note: Filters created using this method are the basis for creating more complex filters. Where you wish to create complex filters a combination or basic filters and Combining filters will be required.

Combining filters

Follow these steps to combine several simple filters and create a more complex filter.

Step	Action
1	Click **Combine**. **Result:** The Combine Filters screen will open. 

Step	Action
2	In the **Filter Name** field, enter a name for the filter.
	Note: This name may be up to 20 characters in length and must be unique for the user.
3	If appropriate, enter a description for the filter in the **Description** field. This field is optional.
4	From the drop down list to the left of the screen, select the first filter use in this combined filter.
5	From the drop down list in the middle of the screen, select the operation that is to be used when combining the two filters.
6	From the drop down list to the right of the screen, select the second filter to use in this combined filter.
7	Click **Save**.
	Result: The changes to the filter are saved.
8	Click **Close** to exit from the screen.
	Result: The combined filter is added to the User Filters list.

Example

If a filter in the form '(A and B) and not C' is required it could be done in the following way.

1. Create three basic filters A, B and C.
2. Combine filters A and B using the combine functionality to create filter X.
3. Combine the new combination filter X with filter C using the 'AND NOT' operation.

Alarm Control

Introduction

The **Alarm Control** tab enables you to change the severity of specific alarms. This permits escalation of severity when an otherwise minor alarm is occurring frequently, indicating a more serious fault. You can change the severity based on:

The description of the alarm

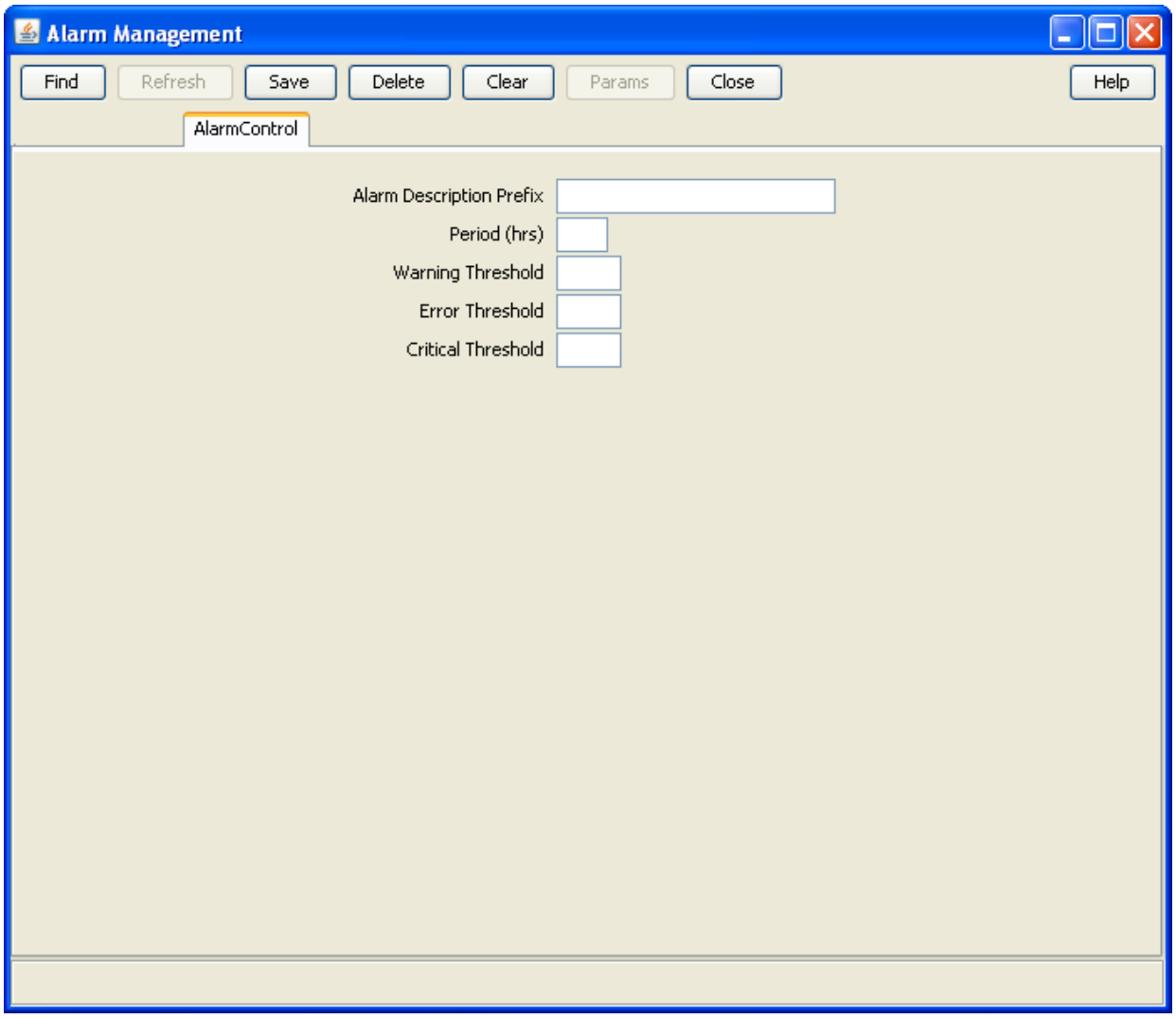
How frequently the alarm is occurring

Important: Rules which change the severity of an alarm must be defined carefully, otherwise important alarms may accidentally have their severity level decreased. This is likely to result in the alarm being missed by the administrators.

Note: If there are more than 20 rules, the performance of the alarm monitoring system may be adversely affected.

Alarm Control tab

Here is an example of the **Alarm Control** tab.



Alarm Control fields

This table describes the function of each field.

Field	Description
Alarm Description Prefix	This field will be searched for in the alarm description. It can either contain the whole alarm description, or the beginning of the alarm description. For more information about the structure of alarms, see *Matching Alarm Message Prefixes* (on page 81).
Period (hrs)	The period used to determine what severity level to set the alarm to. This is calculated in conjunction with the fields.
Warning Threshold	This value is the number of times in the period (set above) an alarm occurs before its severity level is set to warning.
Error Threshold	This value is the number of times in the period (set above) an alarm occurs before its severity level is set to error.

Field	Description
Critical Threshold	This value is the number of times in the period (set above) an alarm occurs before its severity level is set to warning.

Matching Alarm Message Prefixes

The Alarm Message Prefix field forms part of a case-sensitive SQL statement against the SMF_ALARM_MESSAGES table in the SMF database. The statement is a like statement and supports standard Oracle wildcards, including the following:

- % matches any character or sequence of characters
- _ matches any single character

The like statement starts in one of two places in the alarm string:

- The beginning of the SMF_ALARM_MESSAGE record which occurs after the first colon and space
- The beginning of the SMF_ALARM_MESSAGE record

This means that the text entered in the Alarm Message Prefix field will usually match the beginning of either the process name or the alarm text.

Example: If you enter either "smsMaster" or "New", you will match the following alarm (among others):

```
smsMaster(21421) NOTICE: New Connection from 192.168.0.183:36260 accepted (FD 12)
```

Adding Alarm Control rules

Follow these steps to add a new rule to the **Alarm Control** tab.

Step	Action
1	If there is any data in the form fields, click **Clear** to clear it.
2	In the **Alarm Message Prefix** field, enter one of: • The beginning of the alarm description • The full alarm description
3	In the **Period (hrs)** field, enter the number of hours before the alarm count is reset.
4	In the **Warning Threshold** field, enter the number of times the alarm will have to occur before its severity level is set to warning.
5	In the **Error Threshold** field, enter the number of times the alarm will have to occur before its severity level is set to error.
6	In the **Critical Threshold** field, enter the number of times the alarm will have to occur before its severity level is set to critical.
7	Click **Save**. **Result:** The Alarm Control confirmation prompt will appear.
8	Click **OK**. **Result:** The details will be saved to the database.

Note: To set the upper limit of the severity of an alarm, enter a large number in the Threshold field of the severity above the one you wish to set.

Changing an Alarm Control rule

Follow these steps to change the details of a rule in the **Alarm Control** tab.

Step	Action
1	Find the required rule, and bring up its details in the **Alarm Control** tab. See *Using the Find Screens* (on page 12).

Step	Action
2	Change the rule details as required.
3	Click **Save**. **Result:** The changes will be saved to the database.

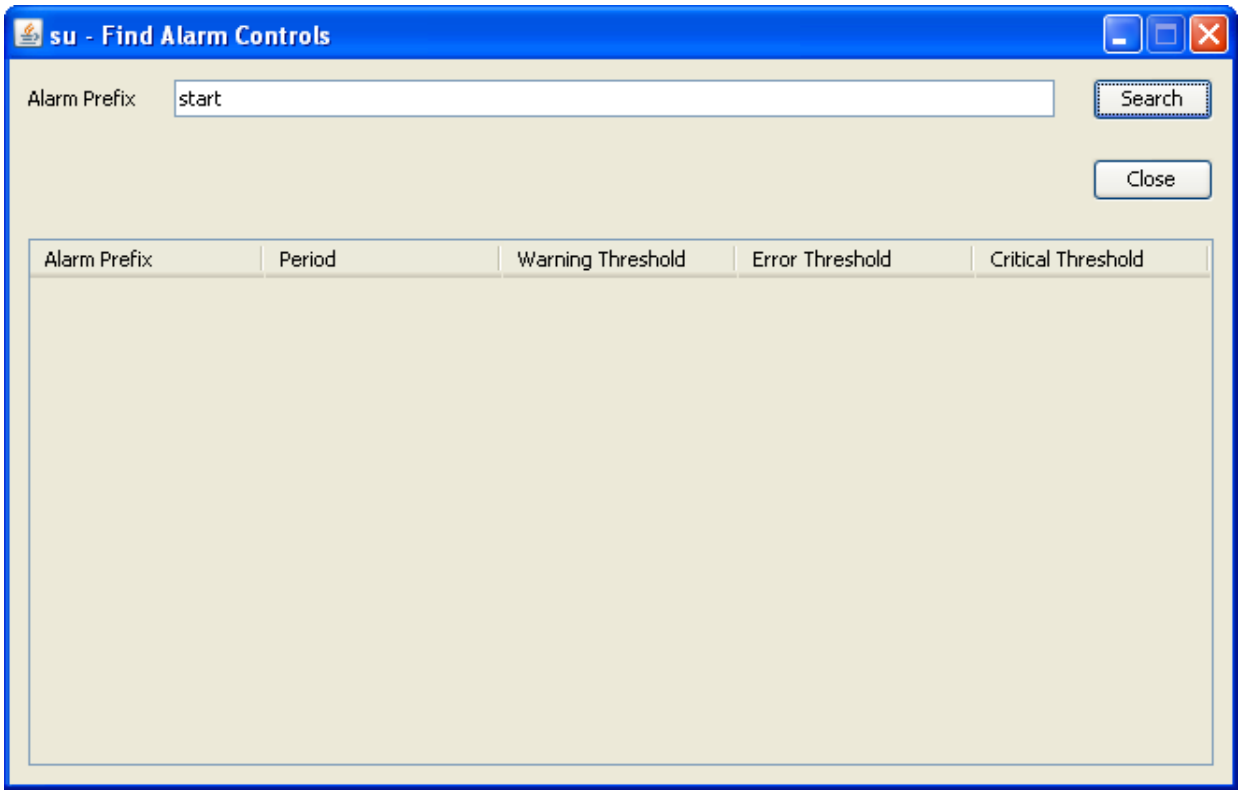
Deleting Alarm Control rules

Follow these steps to delete a rule from the **Alarm Control** tab.

Step	Action
1	Find the required rule, and bring up its details in the **Alarm Control** tab. See *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The Alarm Control confirmation prompt will appear.
3	Click **OK**. **Result:** The record will be deleted from the database.

Find Alarm Control screen

Here is an example of the **Find Alarm Controls** screen, which is used to find alarm control rules.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Alarm Definitions

Introduction

The **Alarm Definition** tab supports the browsing and searching of alarm definitions and the customization of these definitions.

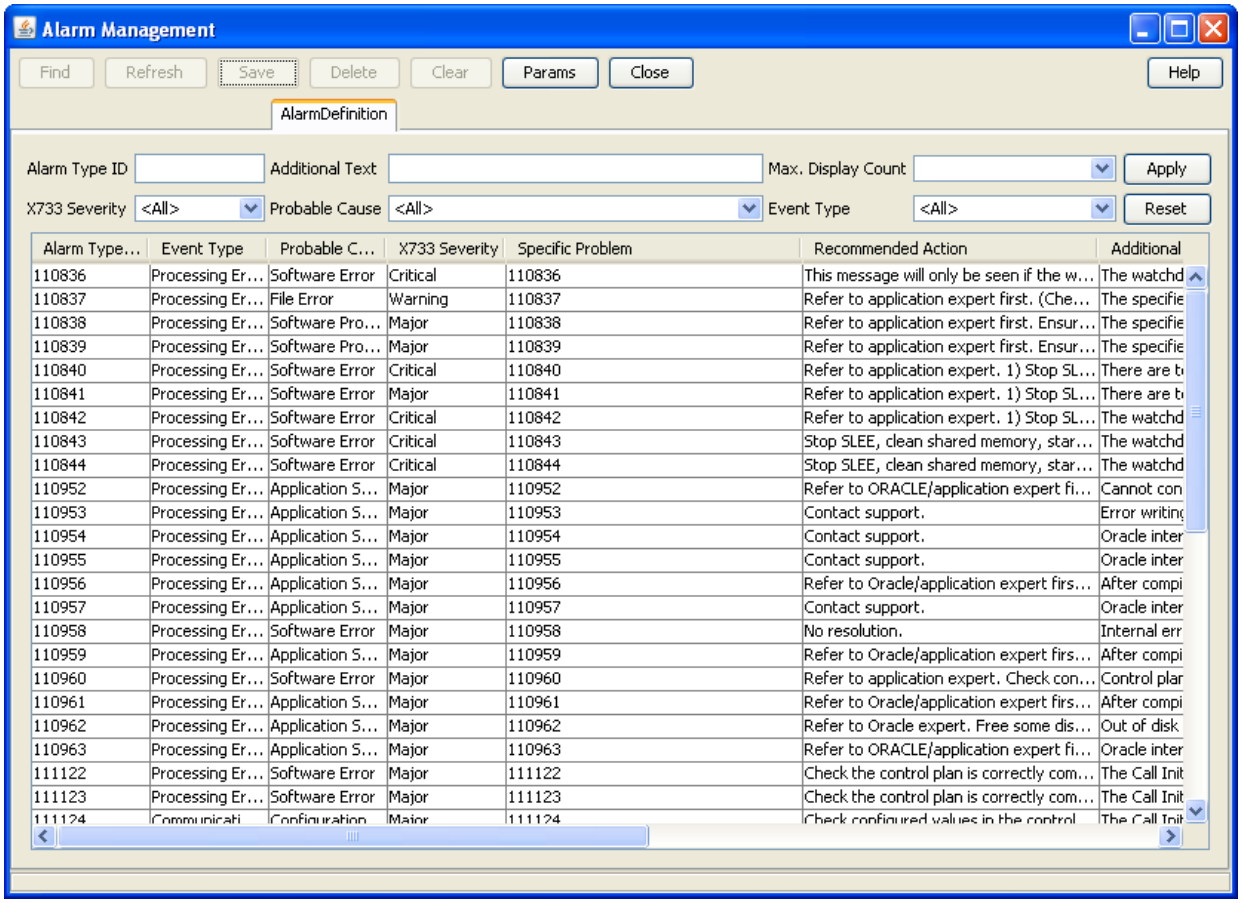
When an alarm is received, it is matched against a set of alarm definitions. These definitions provide the following functionality:

- X.733 definition of the alarm
- Automatic clearance of the alarm
- Automatic clear correlation of alarms
- Alarm suppression
- Recommended action
- Note for operators

Note: Most of this functionality is configurable to meet the operational requirements of a given installation.

Alarm Definition tab

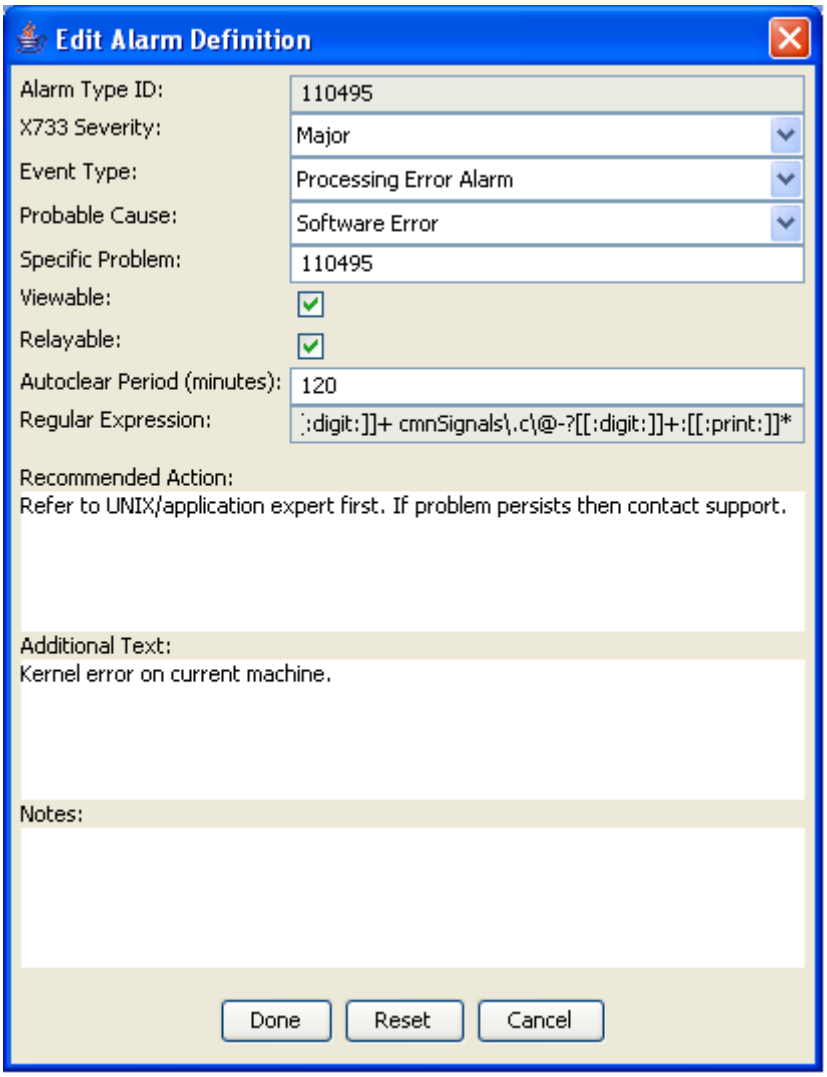
Here is an example of the **Alarm Definition** tab.



Editing alarm definitions

Follow these steps to change the definition details of an alarm. This will change the information that is relayed with an instance of this alarm to an external source and also the information that is shown on the alarm tab for instances of this alarm type.

Step	Action
1	Double click the required alarm in the Alarm table. **Result:** You see the Edit Alarm Definition screen.



2	Add the required information or change the alarm definition fields as required. See *Edit Alarm Definition fields* (on page 85) for more information. **Note:** You can click **Reset** to return the contents of the screen to the original state when the package was installed on the system.
3	Click **Done** to save the changes to the database and close the screen.

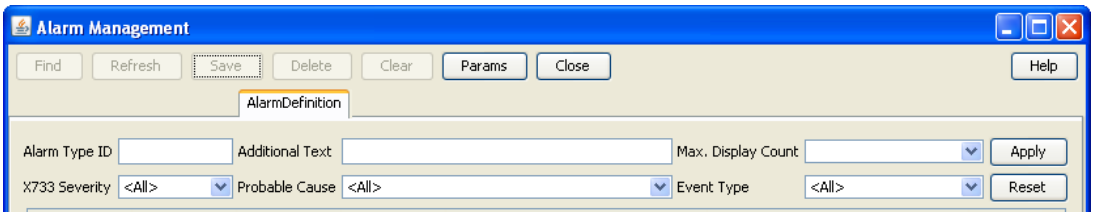
Edit Alarm Definition fields

This table describes the function of each field.

Field	Description
Alarm Type ID	This field displays the unique identifier for this type of alarm. This field is read-only.
Severity	The Oracle severity that alarms of this type will be relayed with. **Note:** This may differ from the severity of the alarm instances that are raised by the system.
Event Type	The event type, which will be one of: • communicationsAlarm • qualityOfServiceAlarm • processingErrorAlarm • equipmentAlarm • environmentAlarm. The event type is attached to alarm instances by the alarm definition and may be changed as required. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Probable Cause	Shows the TMN standard probable causes. It is congruent with the association between event type and probable cause specified in the TMN recommendations (see ITU-T M.3100). The probable cause is attached to alarm instances by the alarm definition and may be changed as required. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Specific Problem	The specific identification of the fault. The Specific Problem is attached to alarm instances by the alarm definition and may be changed as required. This field helps categorize the alarm, allowing quicker identification of the probable cause and recommended action.
Viewable	Indicates if the alarm can be seen.
Relayable	Indicates if the alarm can be relayed.
Autoclear Period (minutes)	The autoclear period determine how long (in minutes) an alarm will be available in the **Alarm** tab, before it is automatically cleared by smsAlarmManager.
Regular Expression	This is the regular expression of the alarm that is raised by the system, and will appear in alarm instances as the alarm description. This may not be changed.
Recommended Action	Describes what action is recommended to resolve all instances of this type of alarm. The recommended action is attached to alarm instances by the alarm definition and may be changed as required.
Additional Text	Any additional text or information about this type of alarm will be entered in this field. The Additional Text is attached to alarm instances by the alarm definition and may be changed as required.
Notes	Any notes about this type of alarm will be entered in this field. The notes text is attached to alarm instances by the alarm definition and may be changed as required.

Using Find Alarm Definitions screen

Follow these steps to sort the alarm definitions displayed in the Alarm Definition table.

Step	Action
1	On the **Alarm Definition** tab, enter the required search criteria. See *Edit Alarm Definition fields* (on page 85) for more information. 
2	Click **Apply** to apply the selected filter. **Result:** The table on the Alarm Definition tab sorts according to the selected criteria.
3	Click **Reset** to clear the Find and return the contents of the screen to the default values. **Result:** The table on the Alarm Definition tab displays all alarm definitions saved in the database.

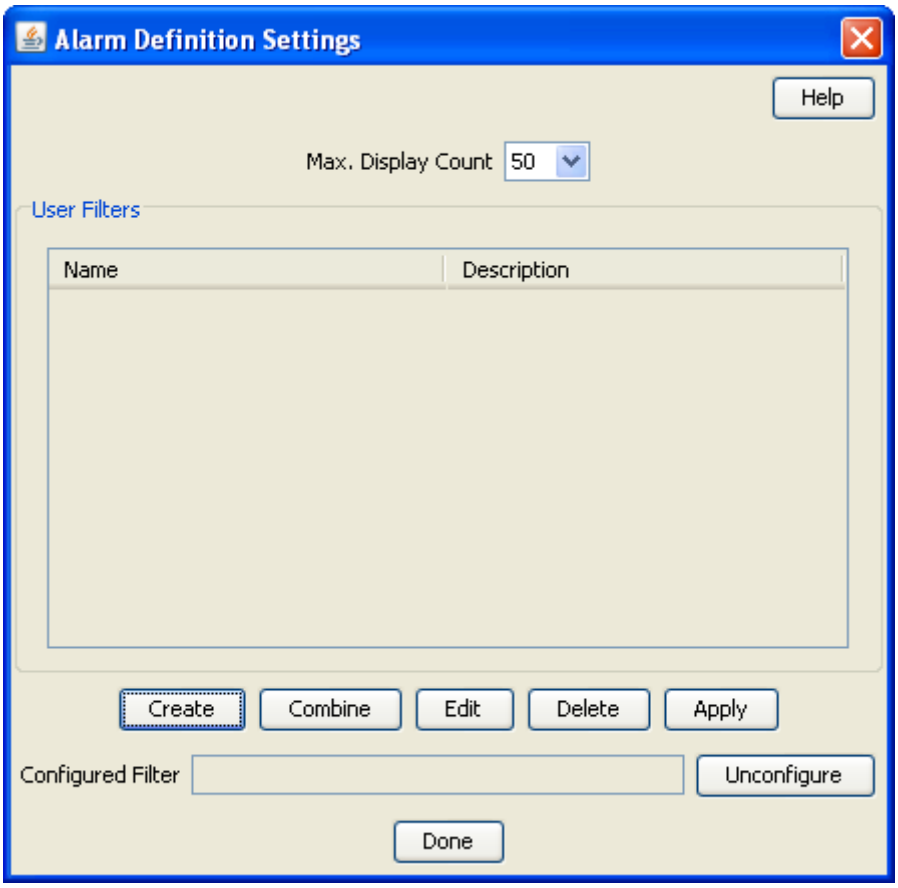
Note: Using the **Alarm Definition** search option will only temporarily filter the records on the Alarm Definition tab. For an advanced filtering options, see *Applying search filters* (on page 86).

Applying search filters

Follow these steps to determine which alarm types are displayed on the **Alarm Definition** tab.

Step	Action
1	From the **Alarm Definition** tab click **Params**. **Result:** The Alarm Definition Settings screen will appear.

Step	Action



2 From the list, select how many alarm definitions that match the configured filter are to be displayed in the **Alarm Definition** tab.

3 Select the filter that is to be used to filter out alarm definitions that are not required. Click **Apply** to apply the selected filter.

Result: The selected filter name will be displayed in the **Configured Filter** field.

4 Click **Done**.

Result: The setting selected will be applied to the alarm definitions and only those that match the set filter and display count will be displayed on the **Alarm Definition** tab.

Alarm Definition Settings fields

This table describes the function of each field.

Field	Description
Display Count	Determines the number of alarm definitions that will be displayed in the **Alarm Definition** tab.
Name	Name given to the filter
Description	Textual description of the filter
Create	Use this button to create a new filter. **Result:** The Create Filter screen appears. For details on using this screen, see *Creating a standard filter* (on page 67).

Field	Description
Combine	Use this button to create a new filter by combining two existing filters. **Result:** The Combine Filters screen appears. For details on using this screen, see *Combining filters* (on page 70).
Edit	Use this button to edit the selected filter. **Note:** This button will open either the Combine Filters screen or the Create Filter screen, according to the way the filter was created.
Delete	Use this button to delete the selected filter.
Apply	Use this button to apply the selected filter to the alarms. **Result:** Only the alarms that match the applied filter will be displayed in the table on the **Alarm Definition** tab of the Alarm Management screen. **Note:** You can only apply one filter to the alarms display at any one time. To apply more than one filter, use the Combine function.
Configured Filter	This field displays the name of the filter that is current being applied to the alarm display.
Unconfigure	Use this button to unconfigure the currently applied filter. This will stop all alarm definition filtering, and thus display all alarm definitions until another filter is applied.

Chapter 7

Statistics Management

Overview

Introduction

This chapter explains how to manage statistics thresholds.

Important: While it is possible to change the details of statistics, changing any characteristic other than description is not recommended. If new statistics are required or any deleted, contact Technical Support.

In this chapter

This chapter contains the following topics.

Statistics Management Module

Introduction

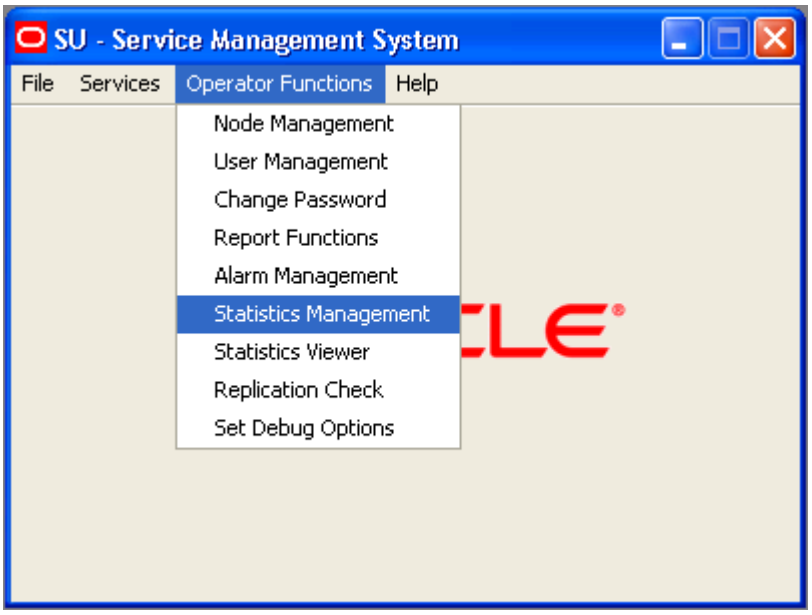
Use the Statistics Management screen to manage statistics thresholds. It contains these tabs:

- *Statistics* (on page 90)
- *Statistics Thresholds* (on page 93)

Accessing the Statistics Management screen

Follow these steps to access the Statistics Management screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action
	
2	Select **Statistics Management**. **Result:** You see the Statistics Management screen.

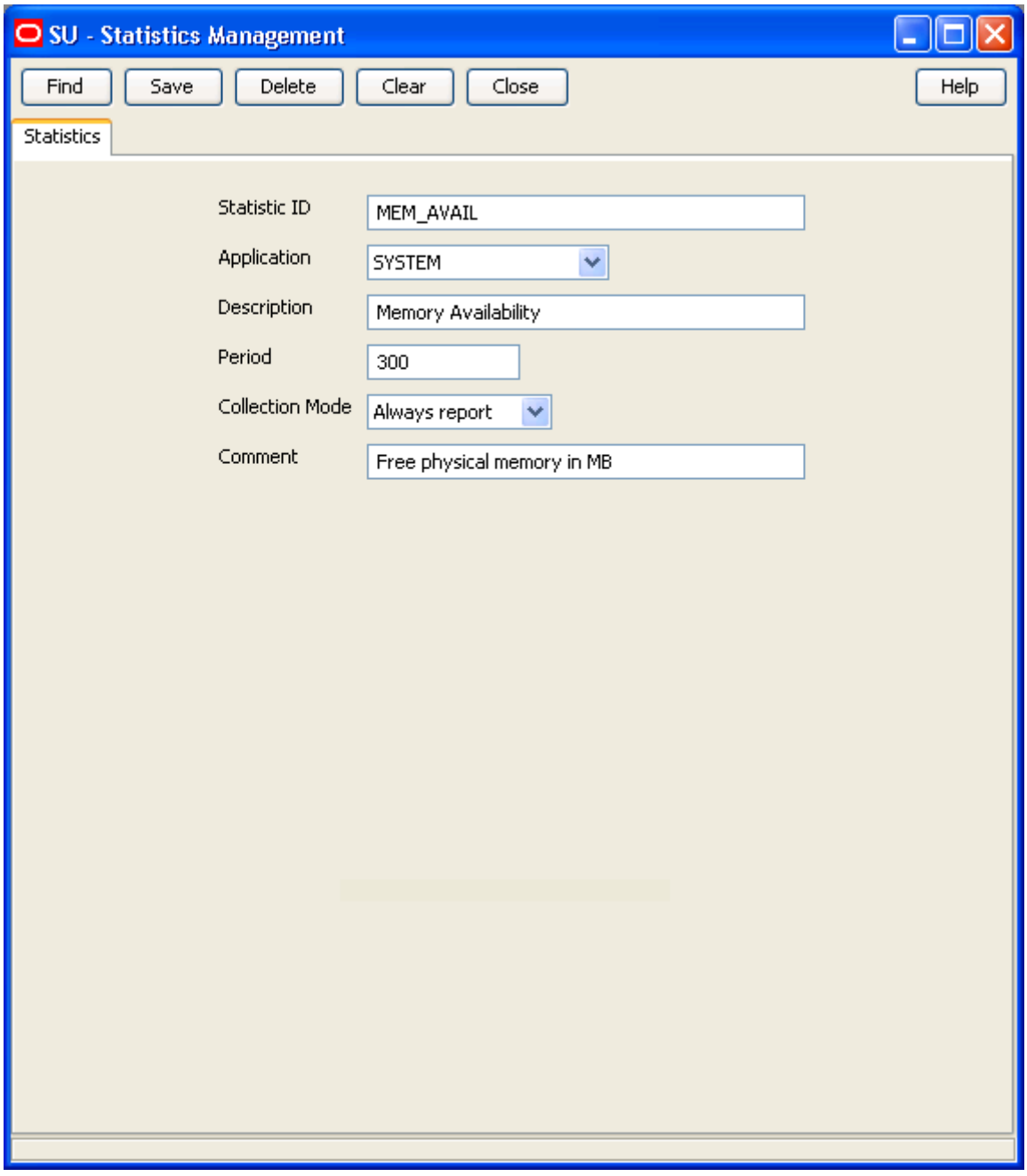
Statistics Management

Introduction

Use the **Statistics** tab of the Statistic Management screen to add, modify, or delete statistics.

Statistics tab

Here is an example of the **Statistics** tab.



Statistics fields

This table describes the function of each field.

Field	Description
Statistic ID	Statistic name. This field is a maximum of 50 alphanumeric characters. (Required.)

Field	Description
Application	Select the application from the drop-down list. **Note:** This list is created from entries in the **eserv.config** file.
Description	Description of the statistic. (Required.) This field is a maximum of 50 alphanumeric characters.
Period	The period in which the statistics is collected, measured in seconds. (Required.) **Note:** For SIGTRAN stack statistics, this must be a minimum of 1 (minute) or a multiple of whole minutes.
Collection Mode	Allows you to control the collection of this statistic. The options include: • Always report • Report non-zero (that is, only report statistics which record events actually occurring) • Never report
Comment	This field is a maximum of 77 alphanumeric characters. (Optional.)

Creating new statistics

Follow these steps to create a new statistic.

Step	Action
1	If the fields on the **Statistics** tab are populated with data, click **Clear**.
2	In the **Statistic ID** field, enter the name of the new statistic.
3	From the **Application** drop down list, select the application. **Note:** This list is created from entries in the **eserv.config** file.
4	In the **Description** field, enter a description of the statistic.
5	From the **Collection Mode** drop down list, select how statistics should be processed.
6	If required, enter any comments about the statistic in the **Comments** field.
7	Click **Save**. **Result:** The details are saved to the database.

Editing and changing statistics

Follow these steps to edit or change a statistic.

Step	Action
1	In the **Statistics** tab, find the required statistic. For more information about finding records, see *Using the Find Screens* (on page 12).
2	Change the details of the statistic as required.
3	Click **Save** **Result:** The changes are saved to the database and you return to the Statistics tab.

Deleting a statistic

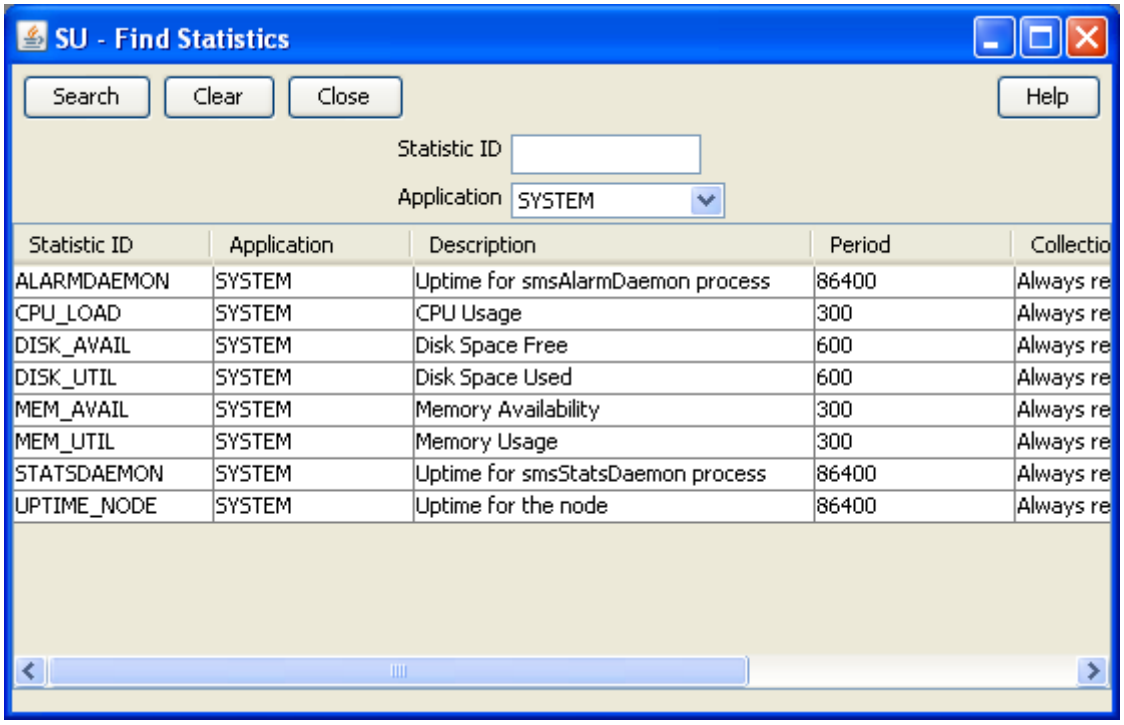
Follow these steps to delete a statistic.

Step	Action
1	In the **Statistics** tab, find the required statistic. For more information about finding records, see *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** You are prompted to confirm the deletion.
3	Click **Yes**. **Result:** The record is deleted.

Note: You cannot delete a statistic if there are references to it within SMS.

Find Statistics screen

Here is an example **Find Statistics** screen.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Setting Statistics Thresholds

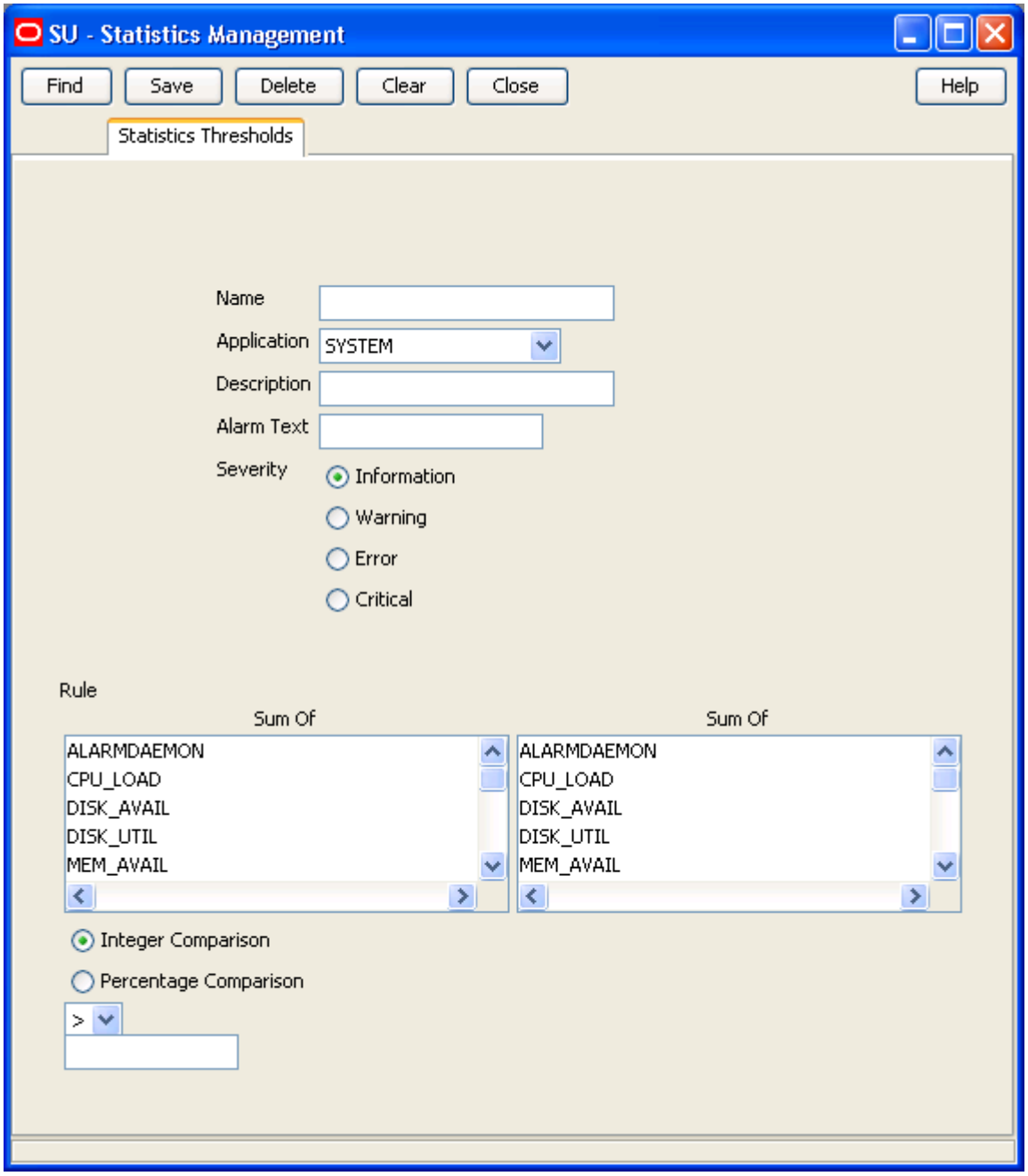
Introduction

Use the **Statistics Thresholds** tab of the Statistics Management screen to set/configure the thresholds of the statistics that are collected.

Every statistic has a value that changes constantly. If the value of the statistic reaches the threshold that you define using these rules, an alarm is generated and sent to the Alarm Management system.

Statistics Thresholds tab

Here is an example **Statistics Thresholds** tab.



Statistics Thresholds fields

The table below describes the function of each field.

Field	Description
Name	Unique identifier for the statistic threshold. This may be up to 50 alphanumeric characters in length and is compulsory.

Field	Description
Application	List of available applications. Displays all applications available for statistics collection.
Description	Description of the statistic threshold rule. This may be up 2000 alphanumeric characters in length.
Alarm Text	Text that is to be displayed in the alarm. This is the text that appears in the alarm when the threshold is reached. The alarm text may be up to 80 characters in length and is compulsory.
Severity	Levels of severity raised when this threshold is reached.
Rule	This set of fields is used to create a threshold rule formula. See the threshold rules below.

Threshold rule format

These are the possible formats of the threshold rules:

```
Column1 - Column2 Operator Value
Column1 - Column2 Operator PercentageStatistic
Column1 Operator Value
Column1 Operator PercentageStatistic
```

Threshold rule fields

Here is description of each field (the percentage and integer fields will only display if the relevant option is chosen).

Parameter	Description
Column1	This column contains a list of statistics created for a particular application. To view the statistics applicable to your application, ensure that the application name appears in the **Application** field. Select one or more statistic in this column by holding down **Ctrl** and clicking on them with the mouse. All Column 1 statistics selected are added together to form a sum total.
Column2	This column contains a list of statistics created for a particular application. It is identical to the statistics displayed in Column 1. Select one or more statistic in this column. All Column 2 statistics selected are added together to form a sum total. The sum total of Column 2 is subtracted from the sum total of Column 1. This column is optional. If this column is empty, no values from this column will be included in the calculation.
Comparison_type	These radio buttons indicate whether the threshold will be against an integer value or a percentage of a system variable.
Operator	The operator is either: • < • > **Note:** The operator disappears if you choose the percentage comparison type, but it is still included in the calculation.

Parameter	Description
Percentage	The percentage and value that the result of Column 1 and 2 results are compared against.
Statistic	If you are using the percentage comparison, this column contains a list of statistics that will be compared against the result of Column 1 and 2.
Value	If you are using the integer comparison, this is the integer value that the result of Column 1 and 2 results are compared against.

Threshold rule examples

Here are two examples of threshold rules.

Example One

A user performs the following steps:

Where: **DISK_AVAIL** is 150 and **DISK_UTIL** is 142.

1 Selects **DISK_AVAIL** statistic from Column 1.
2 Selects **DISK_UTIL** statistic from Column 2.
3 Selects **Integer Comparison**.
4 Selects the **<** operator.
5 Enters the value 10 in the box.

Result:

- System subtracts statistic 2 from statistic 1 (150 – 142).
- Compares the result against the integer value (8 < 10).
- Finds that it is less than 10.
- Generates a statistic notification.

Example Two

A user performs the following steps:

Where: **MEM_UTIL** is 94.00 and **MEM_AVAIL** is 100.00.

1 Selects **MEM_UTIL** statistic from Column 1.
2 Selects the **>** operator.
3 Selects **Percentage Comparison**.
4 Enters the value 90 in the box.
5 Selects **MEM_AVAIL** from the statistic drop down box.

Result:

- System takes the value of statistic 1 (94.00).
- Compares the statistic against the percentage of the value in the drop down box (94.00 > 90.00).
- Finds that it is greater than the resolved percentage value.
- Generates a statistic notification.

Adding a threshold

Follow these steps to add a new statistic threshold.

Step	Action
1	If the fields in the tab are already populated, click **Clear**.
2	In the **Name** field, enter the name of the statistics threshold.

Step	Action
3	From the **Application** drop down list, select the application the statistics will be collected from.
4	In the **Description** field, enter a description of the statistics threshold.
5	In the **Alarm Text** field, enter the text which will appear in the alarm.
6	From the **Severity** options, select the severity of the alarm notification.
7	From the first **Sum Of** box, select either single or multiple statistics. Click on the required statistic or press and hold **Ctrl** down while clicking on each required statistic. You must select at least one statistic from this column.
8	From the second **Sum Of** box, select either single or multiple statistics. Click on the statistic required or press and hold **Ctrl** down while clicking on all statistics required. This column is optional. However, if you select statistics from here, the sum total of these are subtracted from the sum total of the first column. Otherwise this column is not included in the calculation.
9	Select the greater than (>) or less than operator (<). **Note:** The operator disappears if you choose the percentage comparison type, but it is still included in the calculation.
10	If the value you wish to compare against is: • An integer (for example, 10 or 700) select **Integer Comparison** • A percentage (for example, 10%, 100%) select **Percentage Comparison**
11	If you selected: • Integer comparison, go to step 12 • Percentage comparison, go to step 13
12	Enter a value in the box. The result of the rule is compared against the value you enter in this field. Go to step 15. **Example:** (Sum total of statistics 1) - (Sum total of statistics 2) > value
13	Enter a value in the **% of** box.
14	Select another statistic from the drop down box. This enables you to compare the results of the rule against the value of another statistic. **Example:** (Sum total of statistics 1) - (Sum total of statistics 2) < n% of (value of statistic x)
15	Click **Save**. **Result:** The details are saved to the database.

Changing a threshold

Follow these steps to change the statistic threshold:

Step	Action
1	Find the required statistic threshold on the **Statistics Thresholds** tab. See *Using the Find Screens* (on page 12).
2	Change the details of the Statistic Threshold as required. For more information about amending statistics rules, see *Adding a threshold* (on page 96).
3	Click **Save**.

Result: The changes are saved to the database.

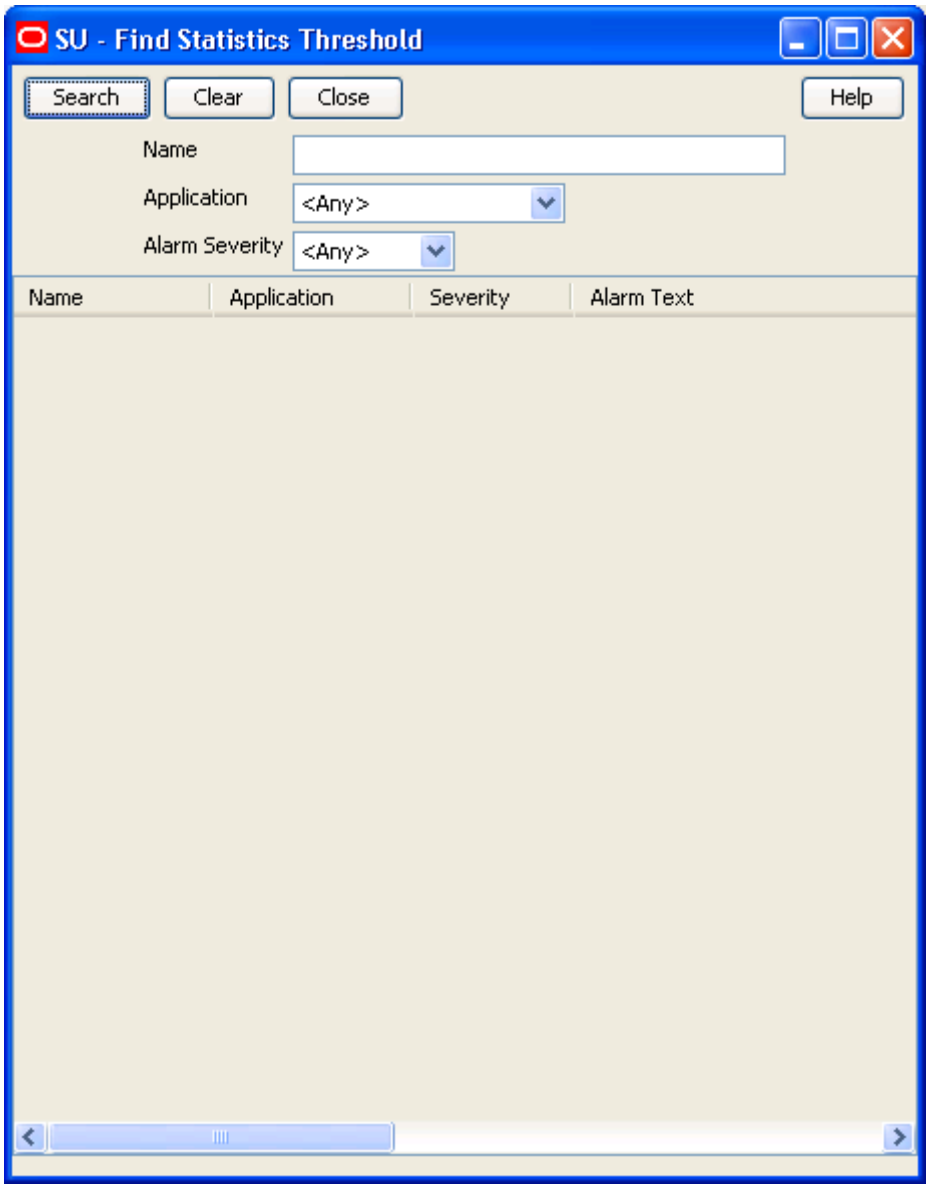
Deleting thresholds

Follow these steps to remove a statistic threshold.

Step	Action
1	Find the required statistic threshold on the **Statistics Thresholds** tab. For more information, see *Using the Find Screens* (on page 12).
2	Click **Delete**. **Result:** The Statistics confirmation prompt appears.
3	Click **OK**. **Result:** The statistics threshold is deleted from the database.

Find Statistics Threshold screen

Here is an example Find Statistics Threshold screen.



For instructions on using the screen, see *Using the Find Screens* (on page 12).

Chapter 8

Statistics Viewer

Overview

Introduction

This chapter explains how to access the statistics viewer and describes the features of the screen.

In this chapter

This chapter contains the following topics.

Statistics Viewer Module

Introduction

The Statistics Viewer screen shows a list of the monitored statistics and allows the list to be edited. A default list of statistics to show are configured. It contains these tabs:

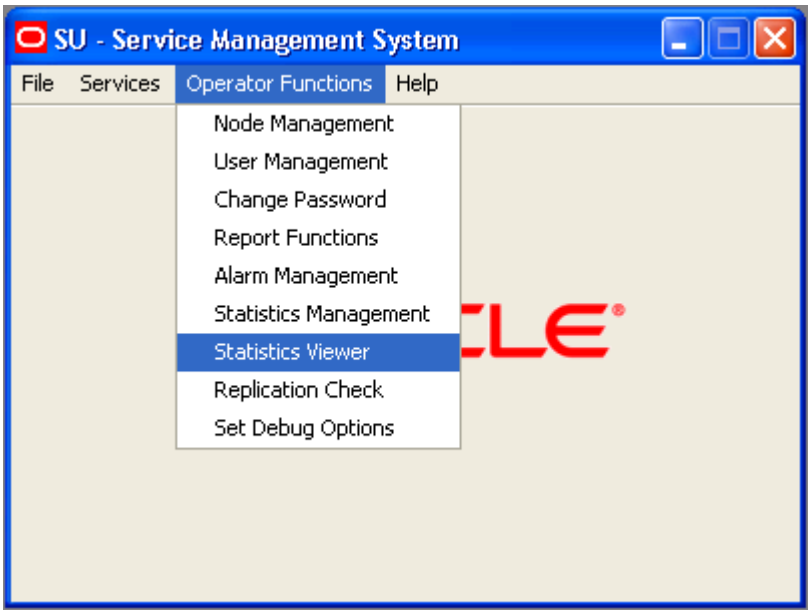
- *Configure Statistics* (on page 102)
- *View Statistics* (on page 106)

Accessing the Statistics Viewer screen

Follow these steps to access the Statistics Viewer screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



2 Select **Statistics Viewer**.

Result: You see the Statistics Viewer screen.

Configuring Statistics

Introduction

Use the **Configure Statistics** tab of the Statistics Viewer screen to add, edit, and delete system statistics. Available system statistics are managed through the statistics management screens.

Each line of the table contains the details of a single statistic and the configured warning ranges. The statistic name is taken from the statistic definitions in the SMF database. The minimum and maximum values for each range are entered by the user.

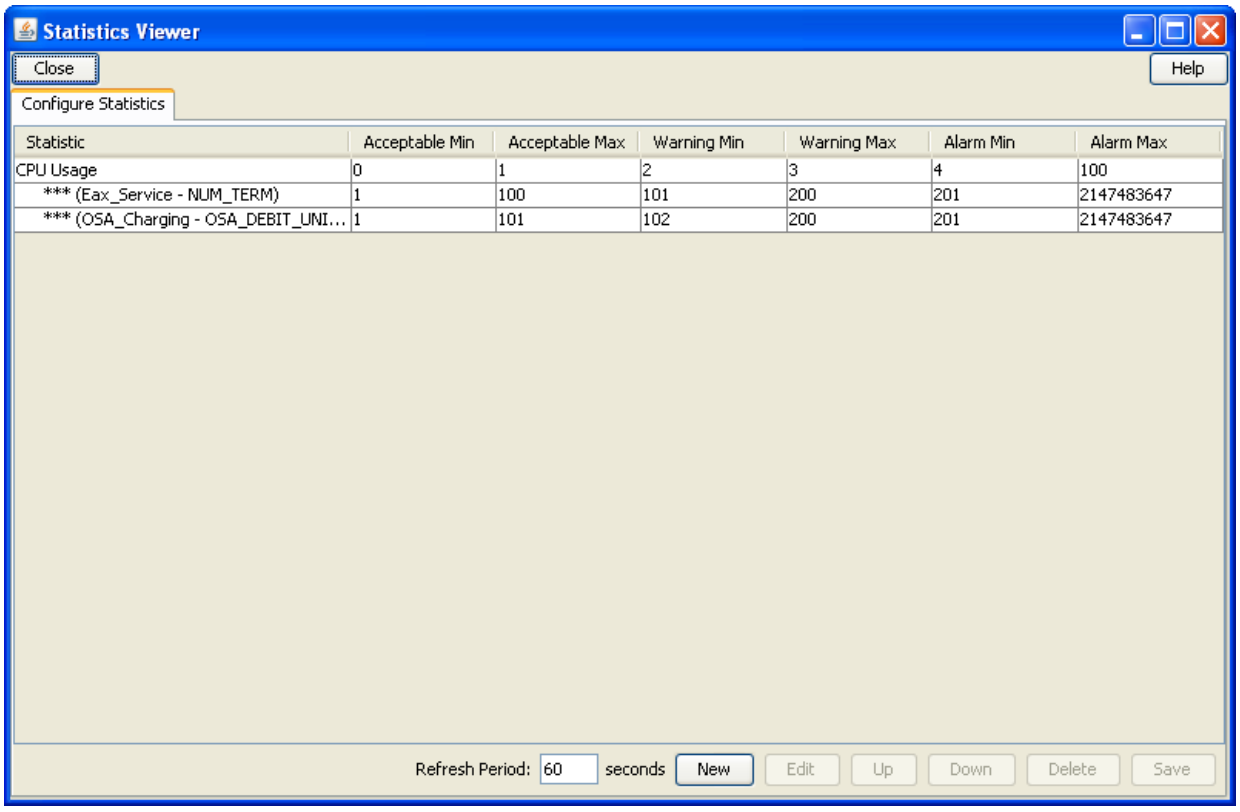
SMS statistics are simply stored as numbers, so the context of the ranges needs to be determined by the user. In the example data, the statistics are all percentages, but other statistics might count the number of certain events or measure absolute amounts (for example, disk usage in KB).

The statistics settings are stored in a database table in the SMF and queried when the screen is loaded. This allows the same statistics to be monitored across different SMS screen sessions.

Note: The configuration is a global configuration, and not a per-user one.

Configure Statistics tab

Here is an example of the **Configure Statistics** tab.



Configure Statistics fields

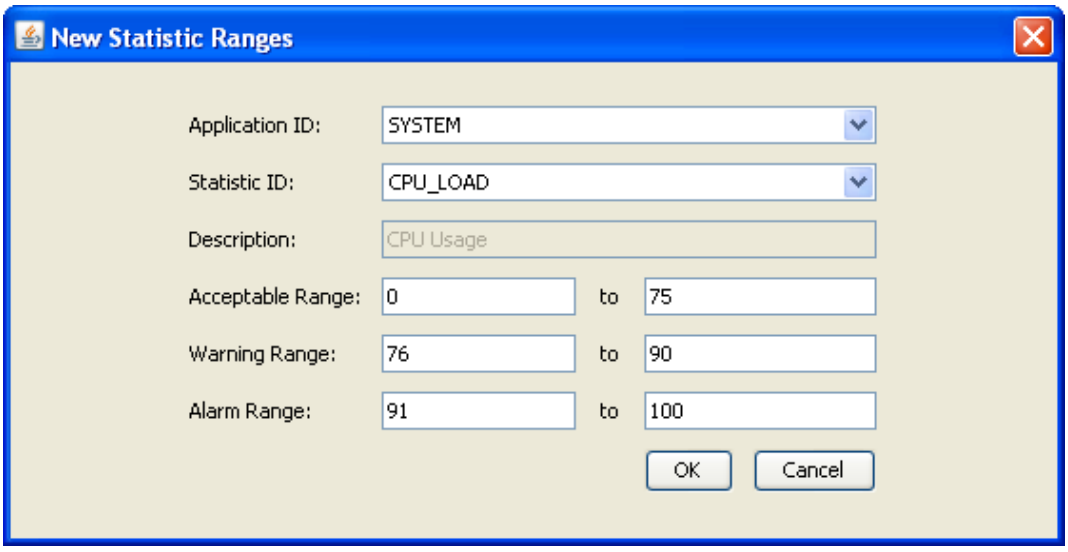
This table describes the function of each field.

Field	Description
Refresh Period	The number of seconds before the screens refresh the statistics display from the database. Defaults to 60 seconds. **Allowed values:** • 60-9999 **Note:** If the refresh period is shorter than the period used by the system utilities to generate and store the statistics, not all refreshes show changes.

Adding a new statistic

Follow these steps to add a statistic.

Step	Action
1	In the **Configure Statistics** tab, click **New**. **Result:** The New Statistic Ranges screen displays.

Step	Action
	

2 From the **Application ID:** drop down box, select the application that the required statistic is for.

The items in this list are read from the database and can be added, edited, and deleted through the Statistics Maintenance screens. For more information, see *Creating Statistics* (on page 90).

3 From the **Statistic ID:** drop down box, select the required statistic.

Result: The statistic name appears in the Description field.

The items in this list are read from the database and can be added, edited, and deleted through the Statistics Maintenance screens. For more information, see *Creating Statistics* (on page 90).

4 In the left **Acceptable Range** field, enter the minimum value for the range. In the right Acceptable Range field, enter the maximum value for the range.

Note: Ensure that this range does not overlap with the Warning Range or the Alarm Range.

5 In the left **Warning Range** field, enter the minimum value for the range. In the right Warning Range field, enter the maximum value for the range.

Note: Ensure that this range does not overlap with the Acceptable Range or the Alarm Range.

6 In the left **Alarm Range** field, enter the minimum value for the range. In the right Alarm Range field, enter the maximum value for the range.

Note: Ensure that this range does not overlap with the Acceptable Range or the Warning Range.

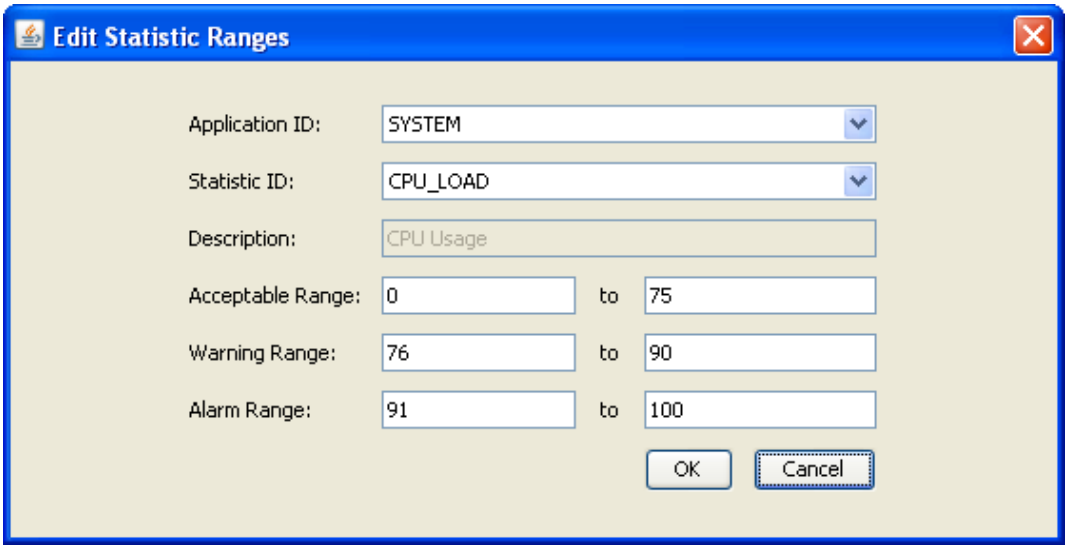
7 Click **OK** to save the details as a new row in the table on the Configure Check screen and close the screen.

Editing a statistic

Follow these steps to edit an existing statistic.

Step	Action
1	From the **Configure Statistics** tab, select the required statistic and click **Edit**.

Step	Action
	Result: The Edit Statistic Ranges screen appears and displays the record's details.



Note: The Statistic description becomes disabled and cannot be edited.

2 Make the necessary edit in the Acceptable, Warning, and Alarm ranges. For more information, see *Configure Statistics fields* (on page 103).

3 Click one of the following.

- **OK** to save the details to the statistic in the table on the Configure Check screen and close the screen
- **Cancel** to close the screen without saving the changes.

Deleting a statistic

Follow these steps to delete an existing statistic.

Step	Action
1	From the **Configure Statistics** tab, select the statistic to delete and click **Delete**. **Result:** The confirmation prompt appears.
2	Click **OK** to delete the statistic from the table on the Configure Check screen and close the screen.

Change the order of statistics

Follow these steps to change the order of the statistics.

Step	Action
1	From the **Configure Statistics** tab, select the statistic to move and click **Up** or **Down**. **Result:** The selected statistic moves up or down in the display table.

Viewing Statistics

Introduction

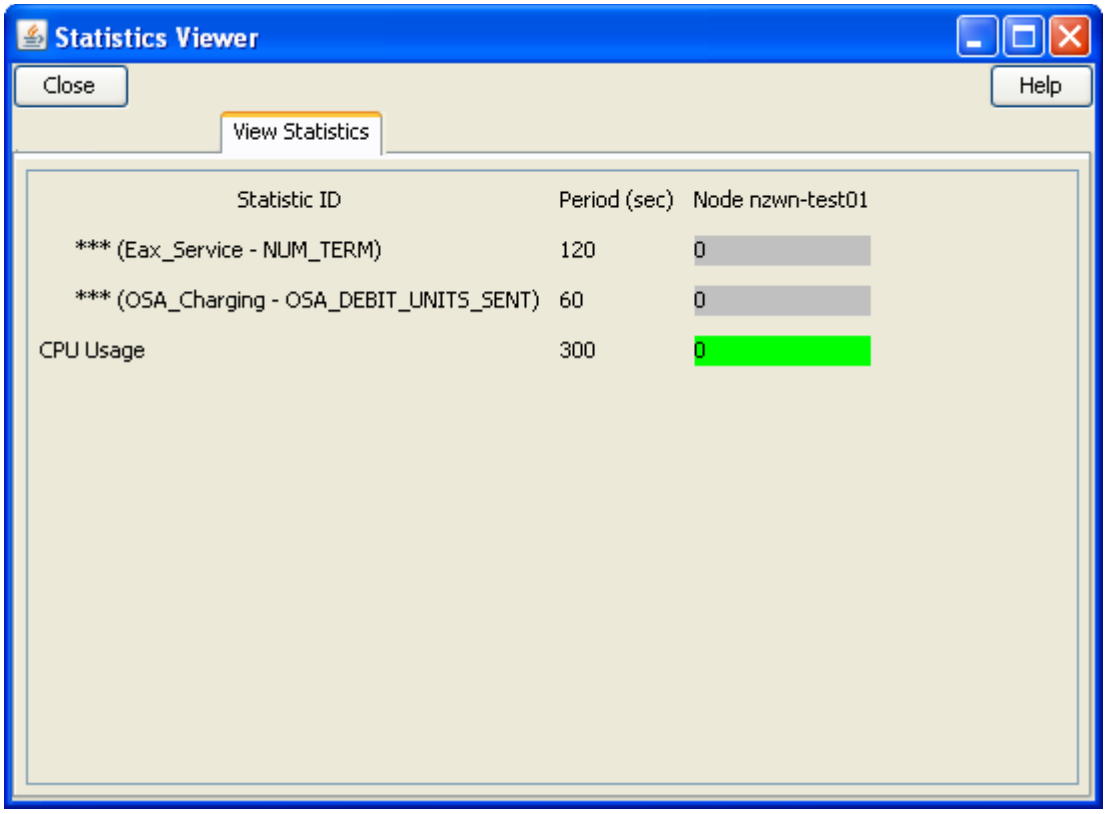
The **View Statistics** tab of the Statistics Viewer screen shows a summary of the monitored statistics for each node.

Each monitored SLC node is listed along the top of the screen. Under each, there is a line for each statistic (in the same order as in the configuration table).

The database is queried periodically to update the displayed values. This period is set in the **Configure Statistics** screen. For more information, see *Configuring Statistics* (on page 102).

View Statistics tab

Here is an example of the **View Statistics** tab.



View Statistics fields

This table describes the function of each field.

Field	Description
Period	The period in which the statistics is collected. For more information, see *Statistics fields* (on page 91).
Node	The node or remote machine from which the statistics are collected. The displayed colors show the configured range for the statistics. For more information, see *Display colors.* (on page 107)

Display colors

This table shows the meaning of the colors displayed in the **View Statistics** tab. The display color of each statistic is determined by the configured ranges.

Colour	Range
Green	The statistic is in the acceptable range.
Yellow	The statistic is in the warning range.
Red	The statistic is in the alarm range.
Neutral	The statistic is not in a defined range.

Chapter 9

The Report Functions

Overview

Introduction

This chapter explains how to access the report functions and describes the features of the screen.

In this chapter

This chapter contains the following topics.

The Report Functions Module

Introduction

The Report Function screen allows you to manage reports. It contains one tab:

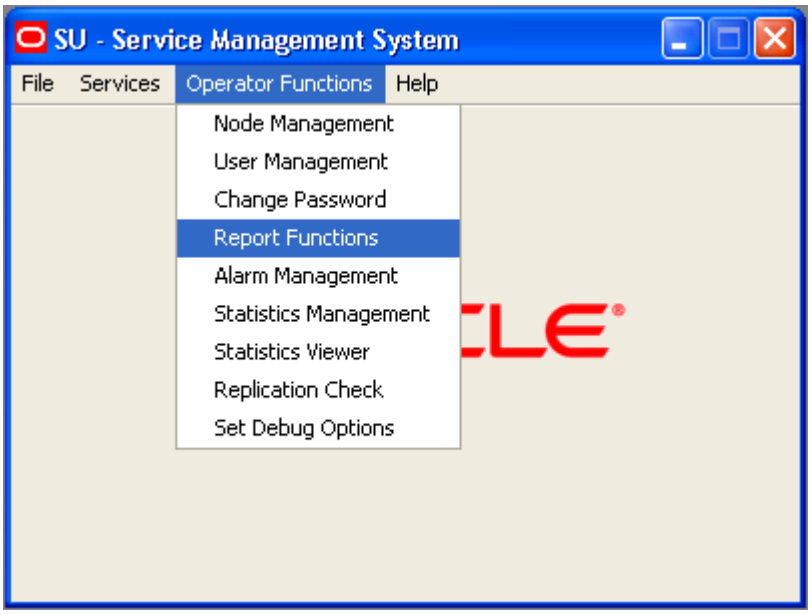
- *Report Selection* (on page 110)

Accessing the Report Functions screen

Follow these steps to access the Report Functions screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



2 Select **Report Functions**.

Result: You see the Report Functions screen.

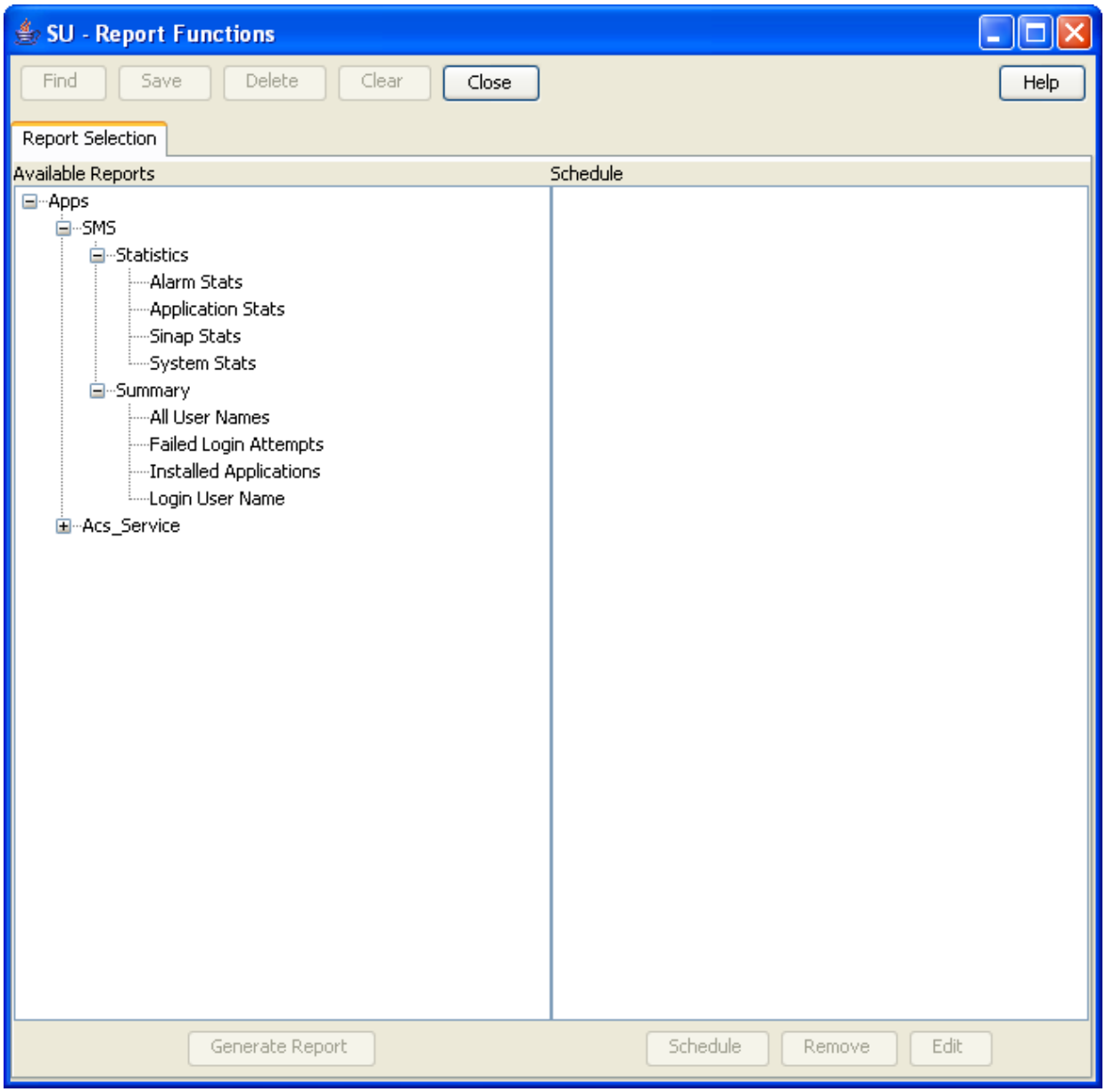
Selecting Reports

Introduction

Use the **Report Selection** tab of the Report Functions screen to view and select the reports that the user has access to.

Report Selection tab

Here is an example **Report Selection** tab.



Report Selection fields

The table below describes the function of each field.

Field	Description
Available Reports	Lists all reports available to the user.
Schedule	Lists all scheduled reports. The schedule for the report lists the frequency and time that the report is scheduled to be generated.

Adding a report to a schedule

Follow these steps to add a new report to the schedule.

Step	Action
1	Expand the list of reports under the **Available Reports** list.
2	Select the report name to schedule.
3	Click **Add**. **Result:** You see the *Report Schedule screen* (on page 114).
4	Add the report schedule using the instructions in *Scheduling Reports* (on page 113). **Result:** The selected report is added to the **Schedule** list.
5	Click **Close**.

Editing a report schedule

Follow these steps to edit a report schedule.

Step	Action
1	Expand the list of reports under the **Available Reports** list.
2	Select the report to edit. **Result:** The details appear in the **Schedule** list.
3	Select the required schedule in the **Schedule** list.
4	Click **Edit**. **Result:** You see the *Report Schedule screen* (on page 114).
5	Edit the report schedule using the instructions in *Scheduling Reports* (on page 113).
6	Click **Close**.

Deleting a report schedule

Follow these steps to delete a report schedule.

Step	Action
1	Expand the list of reports under the **Available Reports** list.
2	Select the report to remove. **Result:** The details appear in the **Schedule** list.
3	Select the required schedule in the **Schedule** list.
4	Click **Delete**. **Result:** The report schedule is deleted from the database.
5	Click **Close**.

Generating a report

Follow these steps to generate a report.

Step	Action
1	Expand the list of reports under the **Available Reports** list.
2	Select the report to generate.
3	Click **Generate Report**. **Result:** You see the Generate Report screen.

Step	Action
4	Generate the report using the instructions in *Generating the Report* (on page 117).
5	Click **Close**.

List of ACS Reports

This table lists the ACS reports.

Report Name	Description
CDR Report	The report shows the ACS CDRs for the specified date range. The report retrieves the information from the processed and received CDR files available in the following directories: • **/IN/service_packages/SMS/cdr/processed** • **/IN/service_packages/SMS/cdr/received**
Customer SN Details	The report generates a list of service numbers and the control plan assigned to the specified ACS service provider name. If ACS service provider name is not specified, the report lists the service numbers and control plans for all ACS service providers.
Customers by FN Set Usage	The report generates a list of feature nodes and the corresponding ACS service provider.
Customers by FN Type Usage	The report generates a list of feature nodes used by each ACS service provider.
Inactive Number Report	The report generates a list of unused ACS service numbers.
Number Addition Report	The report generates a list of ACS service numbers added in a specified date range.
Number Change Report	The report generates a list of ACS service numbers changed in a specified date range.
Number Status report	The report generates a list of ACS service numbers in use or scheduled for use.
Unscheduled Number Report	The report generates a list of unscheduled and not in use ACS service numbers.
Termination Number Report	The report generates a list of ACS termination numbers used by each control plan.
Announcement Usage by Customer	The report generates a list of ACS announcements and the corresponding control plans.
Geography Usage by Customer	The report generates a list of ACS announcement and the corresponding control plans for a specified geography prefix.
Holiday Usage by Customer	The report generates a list of ACS holiday sets and the corresponding control plans.

Scheduling Reports

Introduction

Use the Report Schedule screen to schedule reports that will be automatically generated by the system.

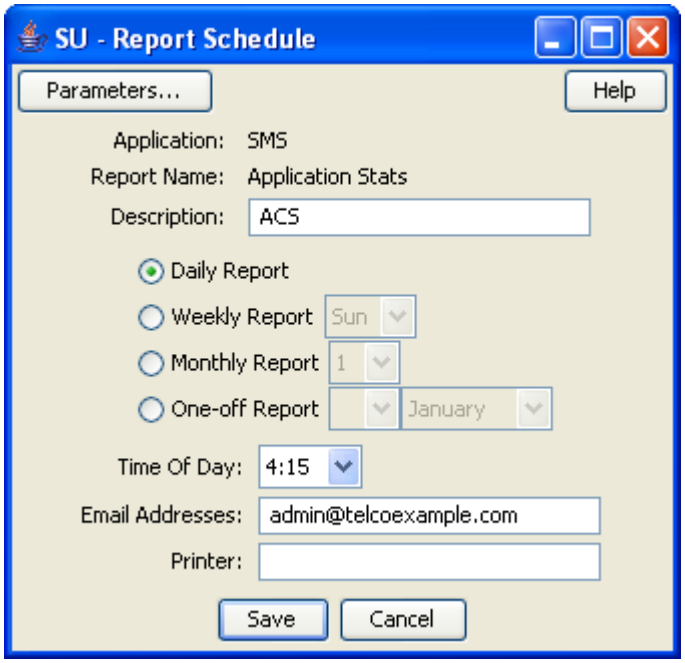
These reports can be delivered by e-mail and/or directed to a printer. Reports are run at the time specified in this screen.

Note: The time and date used is the system date of the SMF database, which is not necessarily the same as the local time of the user scheduling the report.

A scheduled report is generated by the system at the time specified by the selected period (that is, daily, weekly, or monthly) until the Scheduled Report frequency is changed or the scheduled report is deleted.

Report Schedule screen

Here is an example Report Schedule screen.



Report Schedule fields

The table below describes the function of each field.

Field	Description
Application	This field displays the name of application.
Report Name	This field displays the name of the report.
Description	Description of the scheduled report. This may be up to 256 characters in length and is an optional field.
Daily Report	Frequency of report. If this option is selected, the report prints daily at the time displayed in the Time of Day field.
Weekly Report	Frequency of report. If this option is selected, the report prints weekly on the day of the week selected from the drop down list.
Monthly Report	Frequency of report. If this option is selected, the report prints monthly on the day of the month selected from the drop down list.

Field	Description
One-off Report	This type of scheduling is for reports that are only run once at a designated date and time. After a report has run, it is not primary again.
Time of Day	Time of day that the report is generated. This field uses a 24 hour clock format. This list gives the times of day that reports may be generated. The reports may be generated at half-hour intervals throughout the day. If a time is not explicitly selected, the system generates the report at 00:00. **Note:** This time is whatever the local time zone for the SMS machine has been set to. The local time zone value can be configured in **sms.html**. For more information, see *Service Management System Technical Guide*.
Email Addresses	Email address(es) of the person or people who should receive the report. For multiple addresses, separate each e-mail address with a space. The only restriction to this field is the maximum size 256 characters. If the **Printer** field is not filled in, this field is required.
Printer	Enter the full address and name of printer that the report is to be sent to. This printer must be set up on the machine the SMS is running on. If the **Email Addresses** field is not filled in, this field is required.

Changing a schedule

Follow these steps to add or change a schedule.

Step	Action
1	Click **Parameters** on the Report Schedule screen.
2	Enter the parameters using the instructions in *Adding Report Parameters* (on page 116). **Note:** This defines the reporting parameters (that is, what is to be reported).
3	In the **Description** field, enter the description of the schedule.
4	Select the report frequency you require from the report frequency options.
5	If the report frequency is other than daily, select the required date.
6	From the **Time of Day** drop down box, select the time to generate the report.
7	To send reports to an email address, enter the e-mail address in the **Email addresses** field.
8	If you want the report to be sent to a printer, enter the printer address in the **Printer** field.
9	Click **Save**. **Result:** The changes are saved to the database. **Note:** This option appears disabled unless a value is specified in the Email Addresses or Printer fields.

For more information about the fields on this screen, see Report Schedule fields.

Adding Report Parameters

Introduction

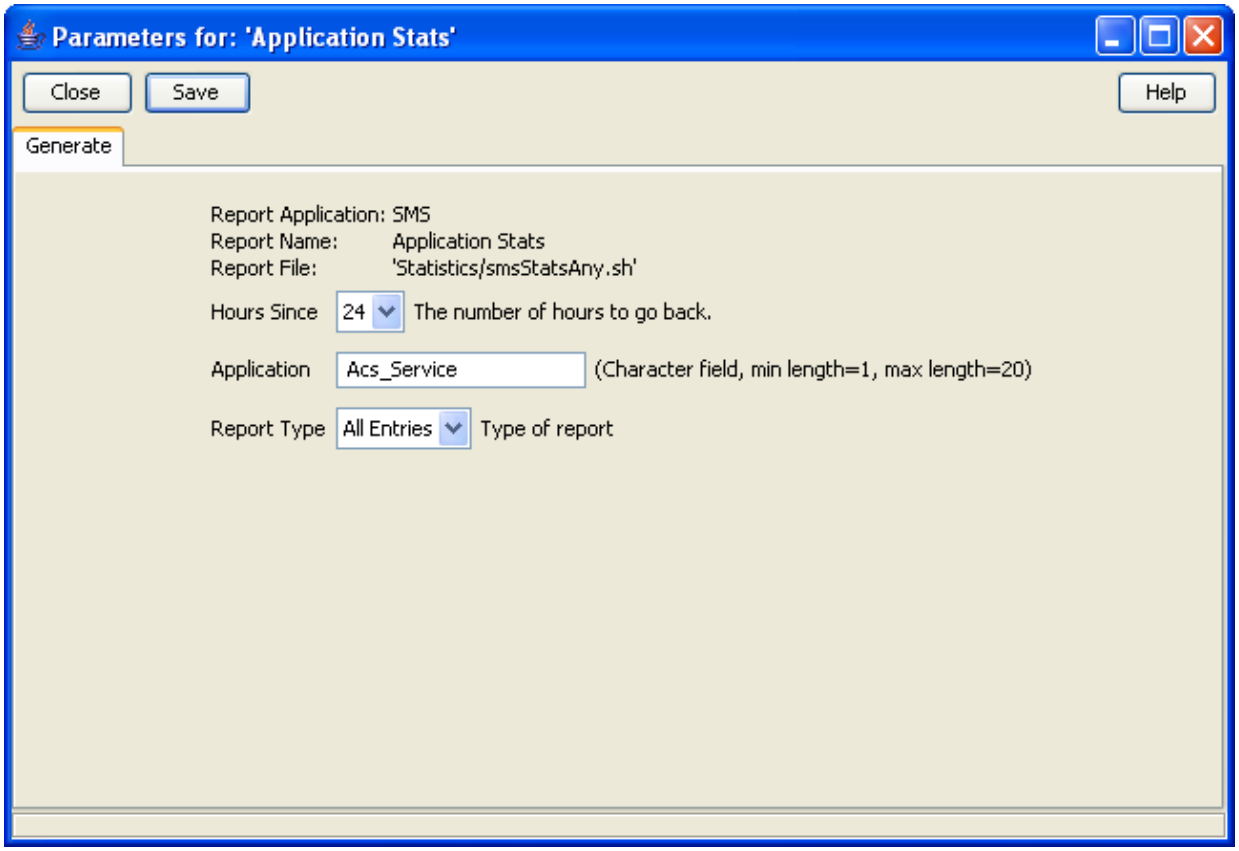
Use the Parameters screen to enter the parameters for reporting (that is, define the applications and statistics to report against).

Accessing the Parameters screen

Access this screen by clicking **Parameters** on the Report Schedule screen.

Parameters screen

Here is an example Parameters for: '*Report_Name*' screen.



Note: The screen displays different fields, depending on the report chosen.

Parameters fields

The table below describes the function of each field for the above example. Different reports display different fields.

Field	Description
Report Application	Name of application (display only).
Report Name	Name of the report (display only).
Report File	Name of the file used to generate the report (display only).

Field	Description
Applications	Name of the applications to report. Report dependent.
Hours Since	Hours to report. Report dependent.
Report Type	Summary or detailed report. Report dependent.

Adding parameters

Follow these steps to add report parameters.

Step	Action
1	Enter the applications to report. Separate each application with a white space.
2	Enter the statistics to report. Separate each statistic with a white space.
3	Enter the hours to report. Separate each hour with a white space.
4	Click **Save**.
	Result: The details are saved to the database.
5	Click **Close**.
	Result: You return to the Report Schedule screen.

Generating the Report

Introduction

Use the **Generate** tab on the Generate Report screen to generate the report.

This screen enables you to enter search parameters for reports that have user definable search parameters. Depending on your operating system, the generated reports are viewable on one of the following:

- On the **Output** tab, which appears next to the **Generate** tab
- In a separate browser window

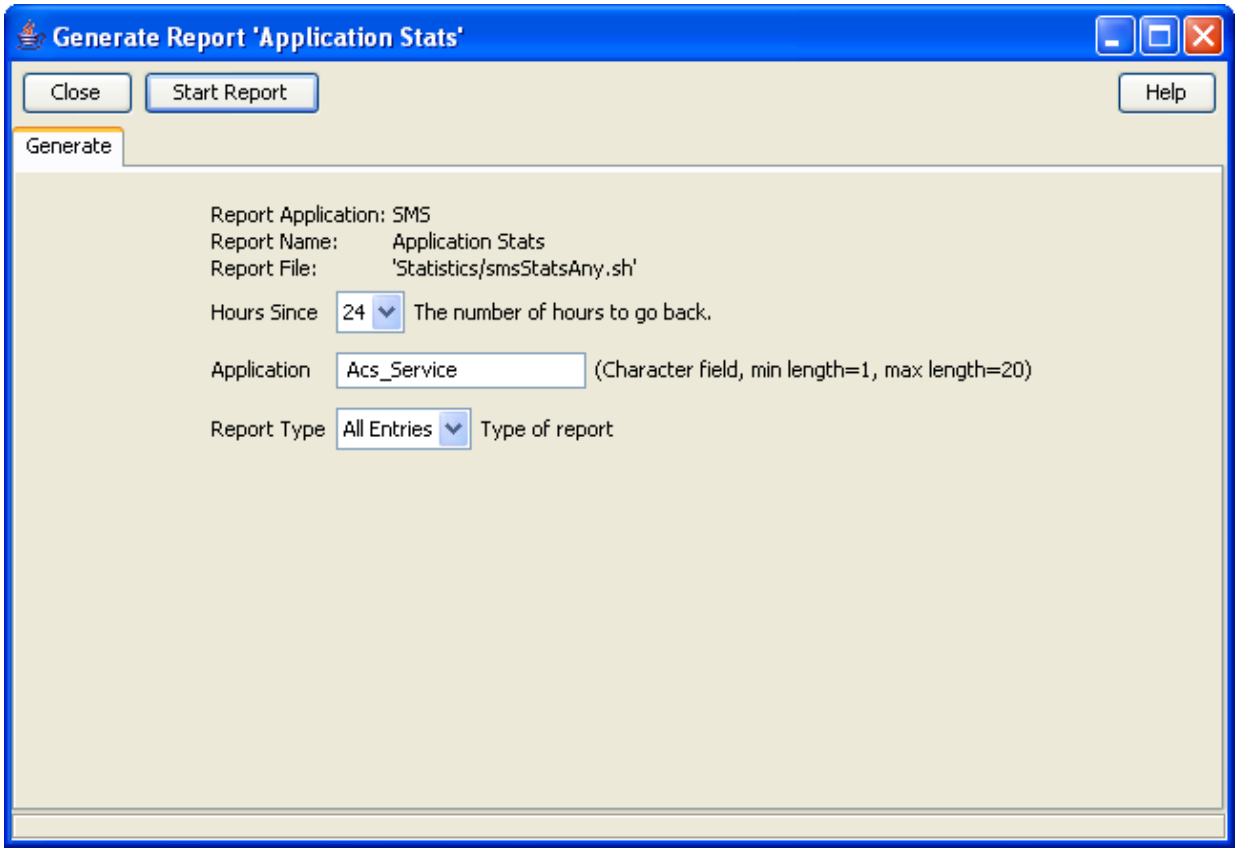
Note: Disable any pop-up blockers before generating reports.

Accessing the Generate Report screen

Access this screen by clicking **Generate Report** on the **Report Selection** tab of the Report Functions screen.

Generate tab

Here is an example **Generate** tab.



Note: The screen displays different fields depending on the report chosen.

Generate fields

The table below describes the function of each field for the above example. Different reports display different fields.

Field	Description
Report Application	Name of application (display only).
Report Name	Name of the report (display only).
Report File	Name of the file used to generate the report (display only).
Applications	Name of application(s) to report. Use any value from the Application field on the **Statistics** tab of the Statistics Management screen.
Report Type	Summary or detailed report. Report dependent.
Hours Since	Hours to report. Report dependent.

Generating and viewing a report

Follow these steps to generate and view a report.

Note: Ensure any pop-up blockers are disabled before generating a report.

Step	Action
1	Enter the report parameters, if required. Separate each parameter in the same field with a white space.
2	Click **Start Report**.
3	Click the **Output** tab.
	Note: Depending on your operating system, the report may appear in a separate browser window instead of on the **Output** tab.
4	View the contents of the report.
5	Click **Save As** to save the contents of the report.
6	Click **Close**.

Chapter 10

Using the Replication Check System

Overview

Introduction

This chapter explains how to access and operate the Replication Check options.

Replication checks enable the user to set up a replication check and then run it.

In this chapter

This chapter contains the following topics.

Replication Check Module

Introduction

The Replication Check System screen allows you to manage reports. It contains two tabs:

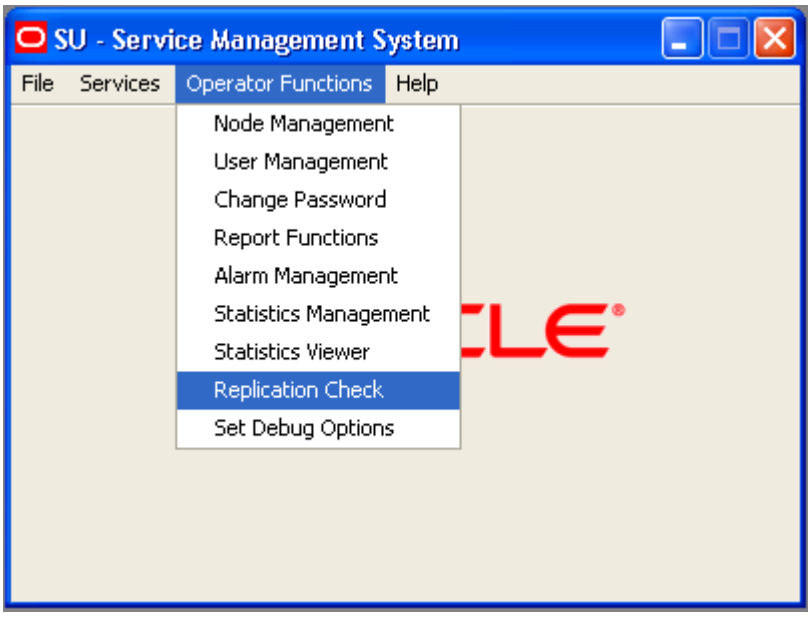
- *Configuring Replication Checks* (on page 122)
- *Viewing Replication Check Reports* (on page 126)

Accessing the Replication Check screen

Follow these steps to access the Replication Check screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



2 Select **Replication Check**, or use the **Ctrl**+**C** shortcut keys.

Result: You see the Replication Check screen.

Configuring Replication Checks

Introduction

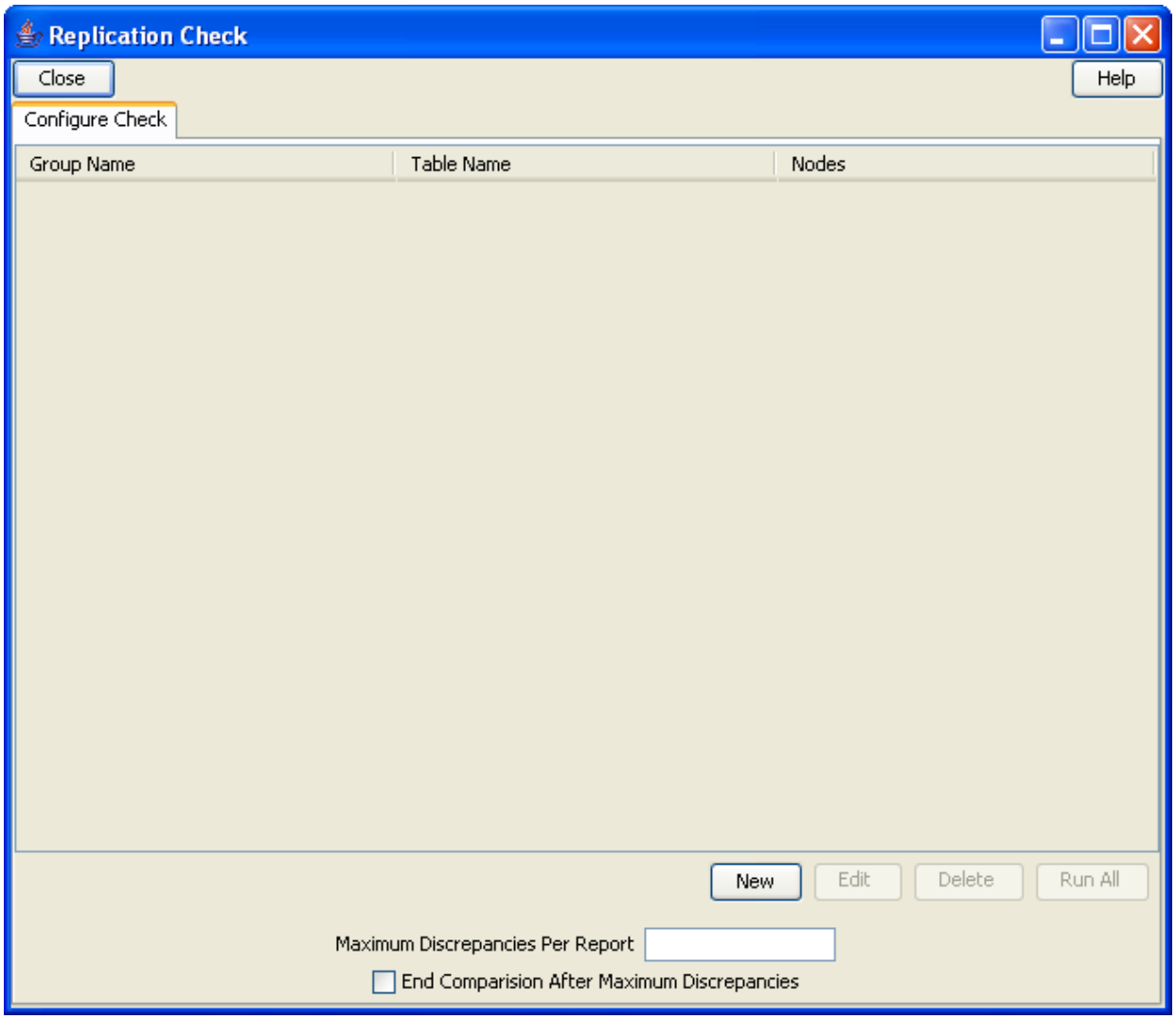
Use the **Configure Check** tab of the Replication Check screen to add, edit, and run replication checks. The replication check definitions are lost when the SMS screens are closed.

It shows a single line (with parameters) for each test. The parameters listed are the name of the replication group, the name of the database table, and the nodes that this test concerns.

On first use, the table does contain any entries. To run a replication check test, you must populate the table with appropriate entries.

Configure Check tab

Here is an example of the **Configure Check** tab.



Configure Check fields

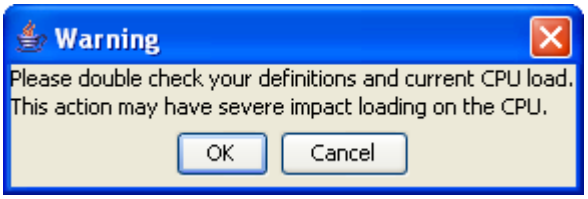
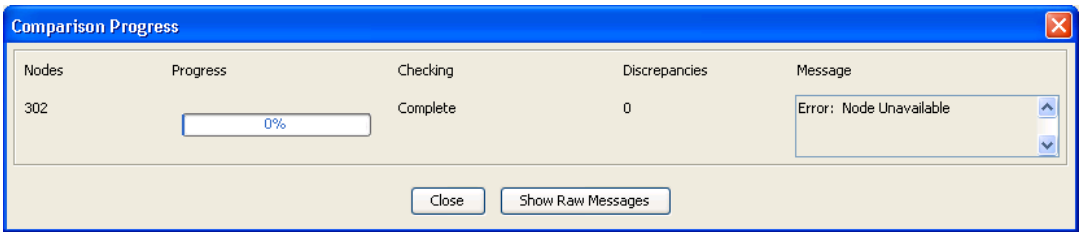
This table describes the function of each field.

Field	Description
Maximum Discrepancies Per Report	Specifies the maximum number of errors reported in the log. If it is left empty, all errors are reported.
End Comparison After Maximum Discrepancies	When checked, the comparison terminates after the maximum number of errors specified in **Maximum Discrepancies Per Report** is reached.

Running replication checks

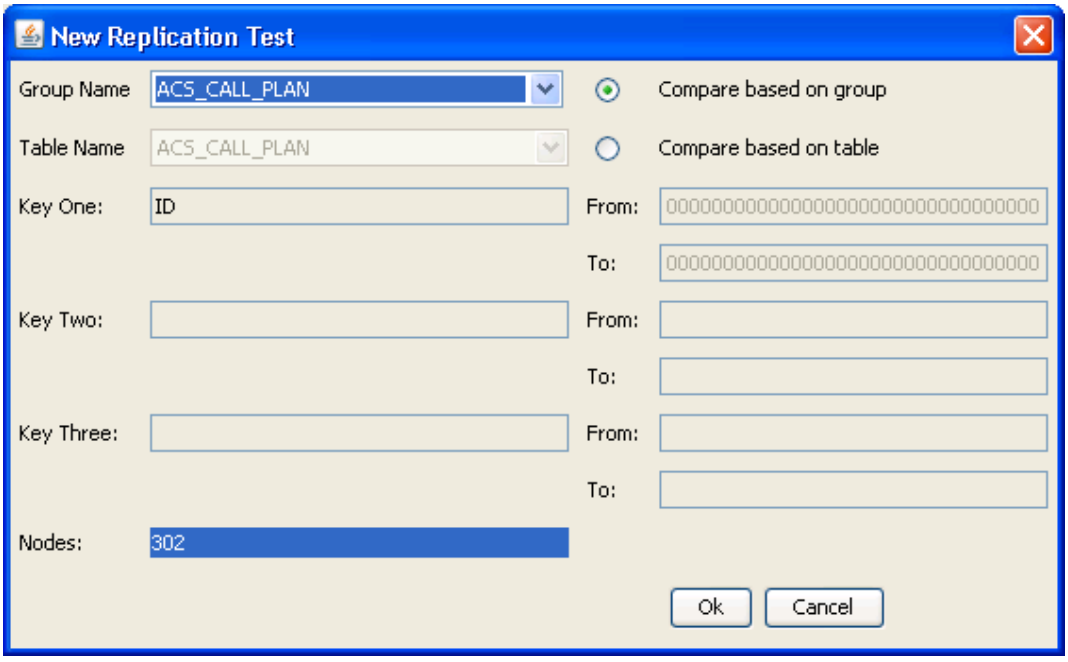
Follow these steps to run the replication checks.

Note: All replication checks described in the table are run at the same time. This can have a serious affect on CPU load and system performance.

Step	Action
1	On the **Configure Check** tab, click **Run All**. **Result:** A Warning dialog box appears and the **Run All** button becomes disabled. 
2	Ensure that you have confirmed your definitions and current CPU load before continuing with this function. To restrict the load created by running the reports: a. Select the **End Comparison After Maximum Discrepancies** check box. b. Enter the maximum number of errors to report in the **Maximum Discrepancies Per Report** field.
3	Click **OK** to continue. **Result:** The replication check starts. The details in the screen are converted into an instruction message, which is sent to the resync/comparison server. The Comparison Progress dialog launches to show the progress of the comparison.  Each node in the comparison has a line with the node number, a progress bar, a status message, and the current number of discrepancies found. The progress bar shows how far through the comparison the node is, in terms of the number of records to be checked. The **Discrepancies** column lists the number of discrepancies found on the SLC so far. Details from the status messages are reported on the screen under the **Message** column. If the server reports an error comparing a node, such as being unable to connect to the client node, this will also be noted here.
4	To see the raw messages, click **Show Raw Messages**. **Result:** The raw messages are displayed, as shown in the example above. To hide the messages, click **Hide Raw Messages**. To cancel the reports, click **Cancel**. **Result:** The comparison/resync server terminates the comparison and it does not finish. The client on the SLC then allows a new connection.
5	After the comparison is finished, **Cancel** is relabeled to **Close**. When you finish running the reports, click **Close**. **Result:** The screen closes and **Run All** becomes enabled again.

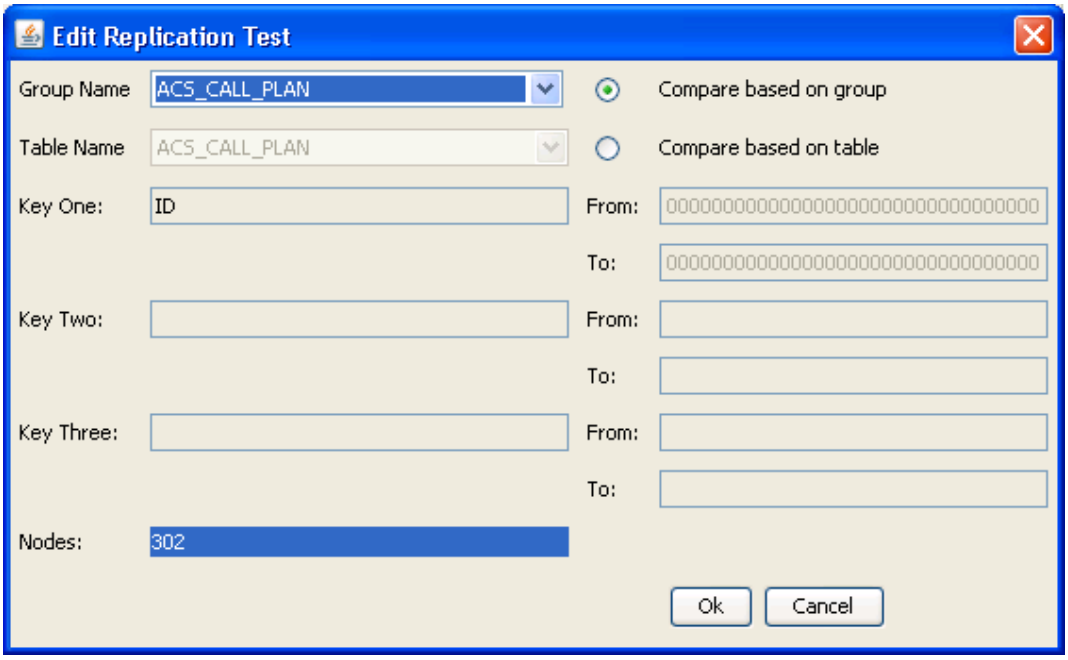
Adding a new replication check

Follow these steps to add a new replication check.

Step	Action
1	On the **Configure Check** tab, click **New**. **Result:** The New Replication Test screen appears. 
2	To compare based on a: • Replication group, select the **Compare based on group** option • Database table, select the **Compare based on table** option **Results:** If Compare based on: • Group is selected, the appropriate table name, primary key names, **From** and **To** values for the primary keys are populated from the definition of that replication group (as defined in the Node Management screen). All these text fields will be disabled. Additionally, the nodes list will have all nodes that the group is replicated to selected by default, though the user can change what is selected. Additionally, the combo boxes and text boxes will be set to grey when disabled, as a visual cue for the user. • Table is selected, a group name is generated (for user reference) and the primary key names are populated. The **From** and **To** values must be entered for each key by the user. Additionally, all selections in the node list will be unselected. The node list is automatically populated from the database and shows all nodes that the chosen group or table is replicated to. The user may select nodes for the comparison to check in the list at the bottom. Multiple selections are allowed by holding down **Ctrl** when selecting.
3	Click **OK** to save the replication test (for use during this session). **Note:** Clicking either button also closes the screen.

Editing a replication check

Follow these steps to edit a replication check.

Step	Action
1	From the **Configure Check** tab, select the replication test to edit and click **Edit**. **Result:** The Edit Replication Test screen appears. 
2	Edit the values as described in *Adding a new replication check* (on page 125).
3	Click **OK** to save the changes and close the screen.

Deleting a replication check

Follow these steps to delete a replication check.

Step	Action
1	From the **Configure Check** tab, select the test to delete.
2	Click **Delete**. **Result:** The Confirm Deletion prompt appears.
3	Click **OK** to delete the test.
	Note: All tests are cleared when the SMS Java screens are closed.

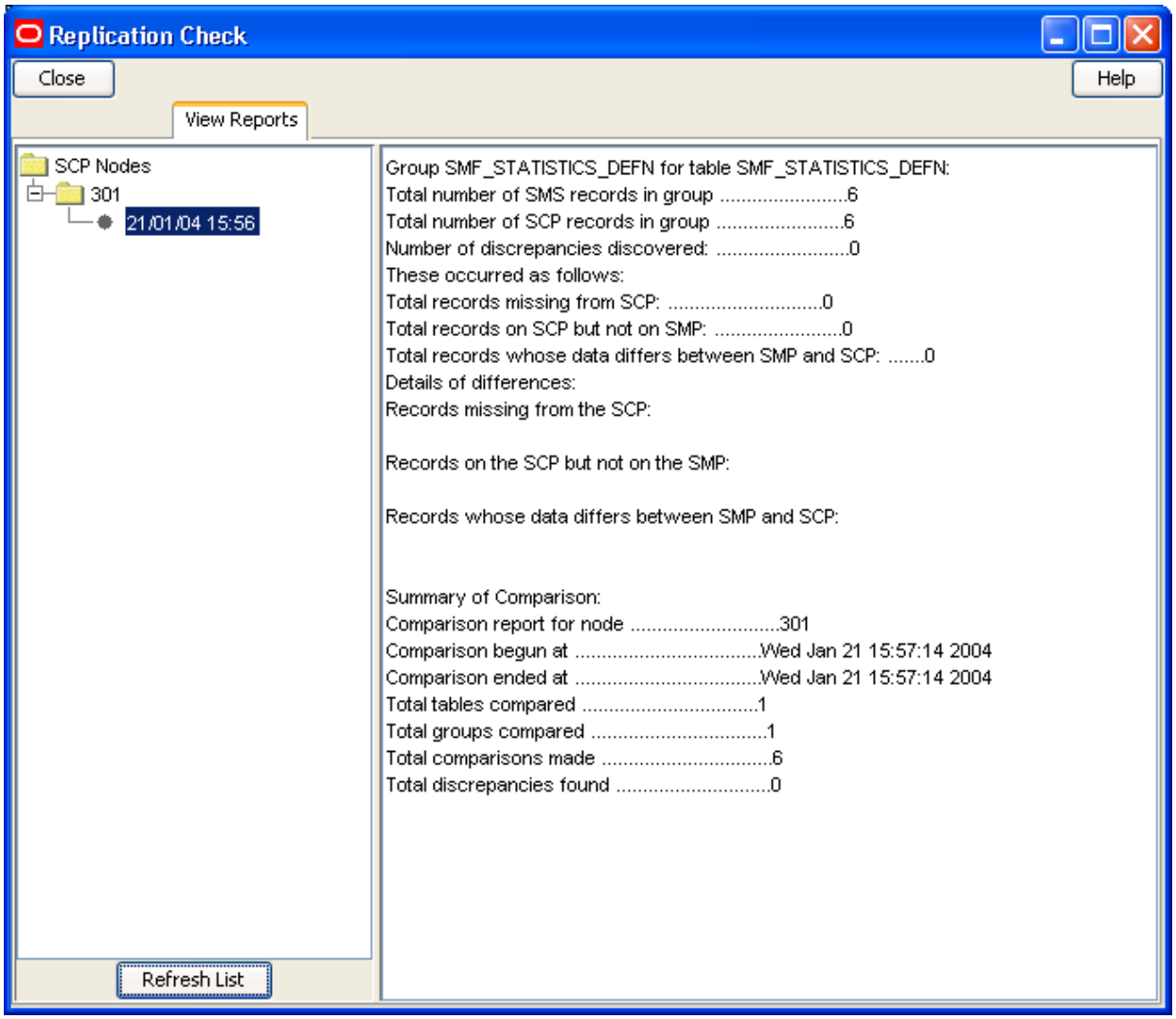
Viewing Replication Check Reports

Introduction

This screen allows you to browse the reports created by the comparison/resync server at the end of each comparison. These reports compare the data held in the SMF database with the data in the specified SLC databases.

View Reports tab

Here is an example of the **View Reports** tab.



View Reports fields

This table describes the function of each field.

Field	Description
left hand area	Shows a list of the replication nodes and reports.
right hand area	Displays the details of the report selected in the left hand area.

Viewing a replication check report

Follow these steps to view a replication check report.

Note: To refresh the list of reports in the left hand area, click **Refresh**.

Step	Action
1	In the **View Reports** tab, select a node from the left hand area. **Result:** The reports for that node are displayed in the left hand area.
2	Select a report. **Result:** The details of the report are displayed in the right hand area.

Chapter 11

Using Set Debug Options

Overview

Introduction

This chapter explains the set debug options function and how to use it.

In this chapter

This chapter contains the following topics.

Set Debug Options

Introduction

Administrators use the set debug options function to enable tracing for Java console and Oracle messages. The tracing options available on this screen are applicable only to the current session.

If tracing is turned on for Java console messages, more information is displayed on the current Java console.

By enabling Oracle tracing, the tracing and timing values of all SQL calls initiated in your current session are written to an Oracle trace file.

Usage:

`$ORACLE_BASE/diag/rdbms/smf/SMF/trace/smf_ora_`*`file_user`*`.trc`

where:

- *`file`* is a number generated by Oracle
- *`user`* is the name of the SMS user

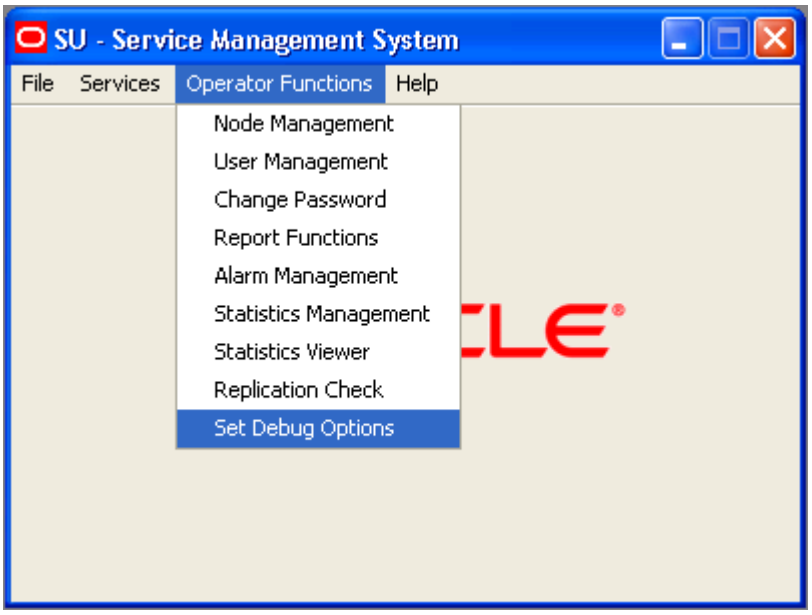
Note: This function is available only to system administrators. Other users cannot view this option on the Service Management System main screen. Enabling Oracle tracing increases the load to the Oracle server, so use this function with care.

Accessing Set Debug Options

Follow these steps to access the Set Debug Options screen.

Step	Action
1	Select the **Operator Functions** menu from the SMS Main screen.

Step	Action



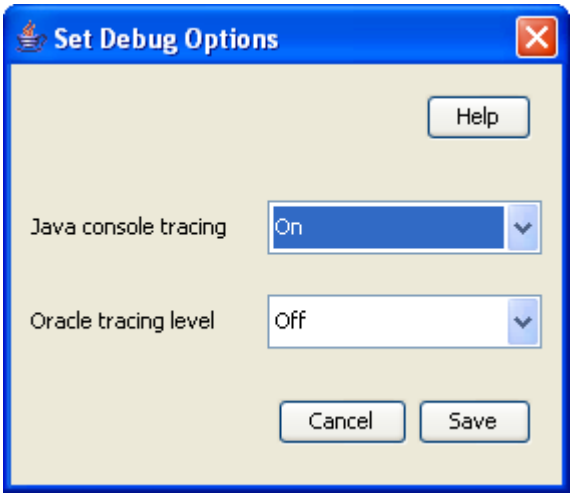
2 Select **Set Debug Options**.

Result: You see the Set Debug Options screen.

Setting debug options

Follow these steps to set up tracing options.

Step	Action
1	Open the Set Debug Options screen. **Result:** You see the Set Debug Options screen.



2 From the **Java console tracing** drop-down menu, select one of the following:

- **On** to enable tracing
- **Off** to disable tracing

Repeat the step for the **Oracle tracing level** drop-down menu.

3 Click **Save** to affect the options.

Chapter 12

Using Help

Overview

Introduction

This chapter explains how to access the help screens.

In this chapter

This chapter contains the following topics.

Accessing Help

Introduction

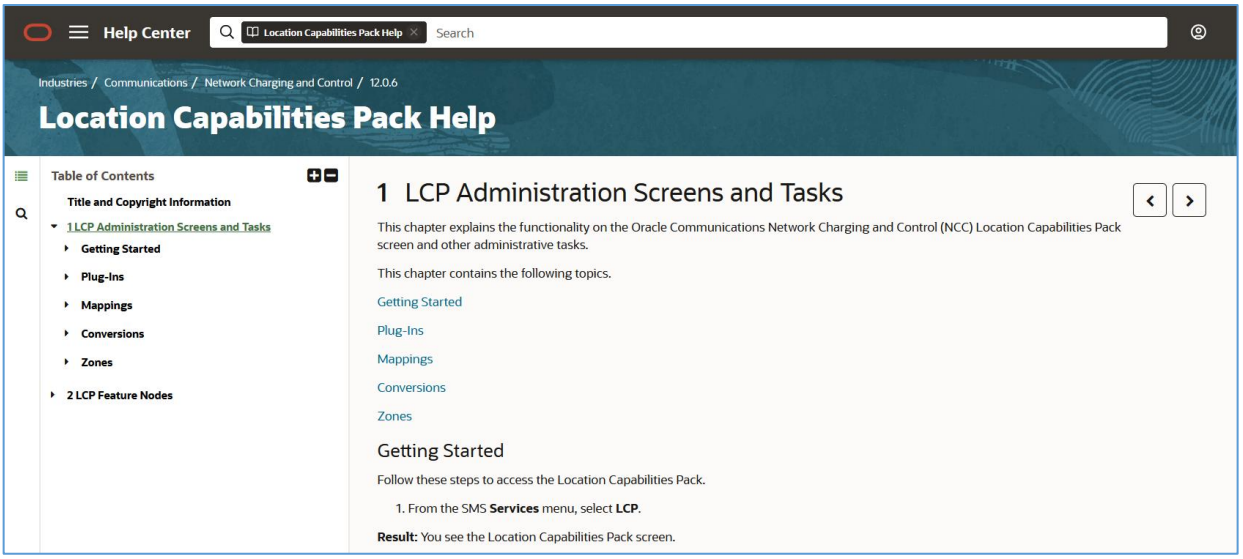
Help screens are available on all screens and tabs. They display information related to the screen from which the help was initiated.

The help information that is given includes descriptions of the fields on the screen and procedures for performing the basic functions of the screen.

Accessing a help screen

To access the help for a screen or tab, click the **Help** button. The Help opens in a web browser.

Here is an example web based Help displayed when you click **Help** on the LCP screen.



Note:

- From version 12.0.6 onwards, web based help is displayed when you click the **Help** button in the SMS UI.
- You can access Help from either SMS UI, or directly from the Oracle Help Centre website. All the Helpsets for 12.0.6 are available at the following location: https://docs.oracle.com/en/industries/communications/network-charging-control/12.0.6/index.html
- You can also use the search functionality provided on this page to search any keyword across multiple Helpsets.