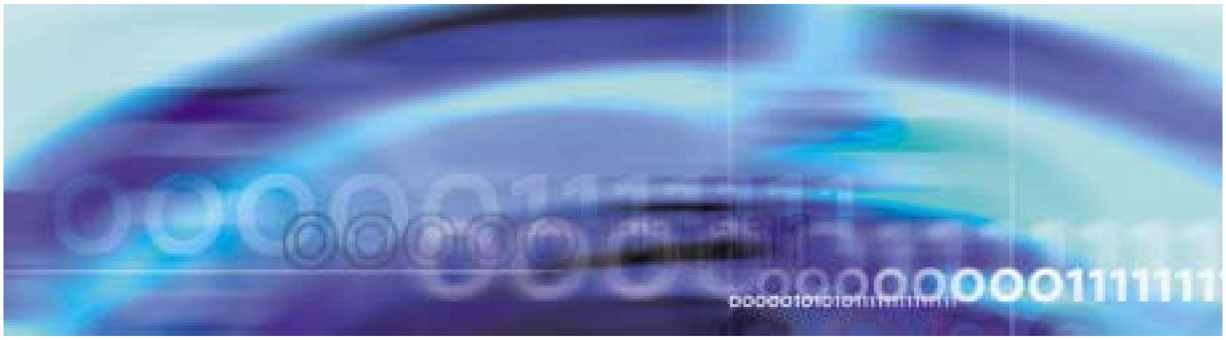


Integrated EMS Security and Administration

Introduction

This section describes the procedures for the security administration of Integrated EMS Client, using Jobs, modifying the Security Notice text displayed at Integrated EMS Client startup and configuring the printer for Integrated EMS Client. This section contains the following sections:

Table of Contents

Integrated EMS Security and Administration 1

Securing Integrated EMS client 7

Configuring user settings 17

Configuring scope and group settings 34

Using custom view scope 46

Using the Operations tree 56

Securing Integrated EMS client

A secure Integrated EMS ensures legitimate use of the network, and maintaining confidentiality, data integrity, and auditing in the network. security management involves identifying assets, threats, and vulnerabilities, and taking protective measures to prevent unauthorized use of computing systems.

Security administration helps you manage the Integrated EMS server security information. This security information is stored in the database and in a configuration file, namely securitydbData.xml in the *<IEMS Home>/conf* directory. These two sets of security information are maintained in synchronization with each other.

You can achieve detailed authorization by setting the scope for the operations assigned to a group. This scope defines the restricted access for the operation in that group. By setting Custom View Scope to groups, users see only the Integrated EMS information necessary for their allocated operations. Setting the Custom View Scope criteria for a group of users to a particular network type, allows the users of that group to view only the nodes of the particular network on which the user is authorized to perform operations. Integrated EMS hierarchy in managing authorization is User - Group - Authorized Scope or Authorized View - Operations.

As soon as a user logs in to the Integrated EMS, the only operation available are those based on the groups to which that user belongs. Therefore, user administration is a prime function for Integrated EMS administrators.

An administrator can authorize users or groups to perform the following operations in the Integrated EMS:

- Providing group-based authorization, where users can be assigned to groups, with configured levels of authorization, in addition to authorizing specific users.
- Providing a detailed access control and access job definitions for Groups, Views, and Operations.
- Limiting the access for some users to specific sub-sets of objects or instances, for example, user access can be limited to a certain type of device.

The security administration tool (an Integrated EMS sub-application), provides facilities for carrying out the above security operations. Using this tool, Integrated EMS administrator can perform the following tasks:

- User-specific tasks
  - Adding new users
  - Associating groups with a user
  - Setting a user profile
  - Changing user password
  - Associating operations to a user
  - Viewing the audit trails
  - Deleting a user
  - Listing all the users
- Group-specific tasks
  - Adding a new group
  - Setting a scope
  - Assigning users to a group
  - Assigning operations to a group
  - Custom view scope settings
  - Organizing the Integrated EMS operations

The following two subsections describe how to get started:

- Starting the Security Administration tool
- Adding New Users

Starting the Security Administration tool

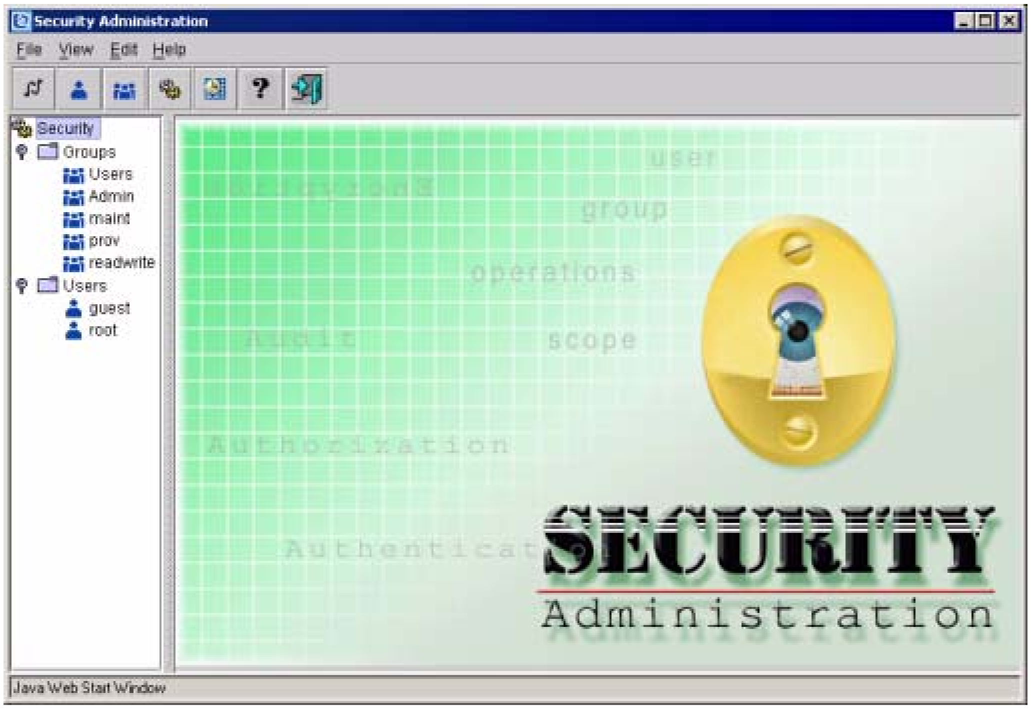
The Security Administration tool is a sub–application of Integrated EMS. You can start this tool only if you are an authorized user. To start the Security Administration tool, follow these steps:

To launch Security Administration tool in the Integrated EMS, follow these steps:

At the Integrated EMS workstation

1. Refer to the "Launching Integrated EMS Java Web Start Client" of the *Integrated EMS Basics*, NN10329-111 to launch the Integrated EMS Client.
2. Select the **Tools-->Security Administration** menu command.

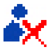
   The Security Administration tool opens, as shown in the following figure:



Note: If the Security tree does not show nodes under the Groups and Users nodes, refresh the Security Administration window using the Refresh tool button.

In the left-hand navigation pane, the Security Administration tool displays the current status of the users using different icons. The following table lists the icons and their meaning

Description of icons in Security Administration tree

Icon	Description
	User account is enabled
	User account is disabled; the user cannot log in until re-enabled.
	User account is expired
	User password is expired; user cannot log in until password changed or existing password re-authorized.
	User forced out of the server (similar status to disabled; the user cannot log in until re-enabled).
	User denied to log in because of continuous unsuccessful log in attempts.

Adding New Users

Adding a new user is a very important activity in providing access to the Integrated EMS Server. Operation and Maintenance personnel can be assigned Integrated EMS views with restricted access to different modules, such as Maps, Fault Management, and other sub-applications.

To add a new centrally-managed user in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the **File-->New-->Add User** menu command

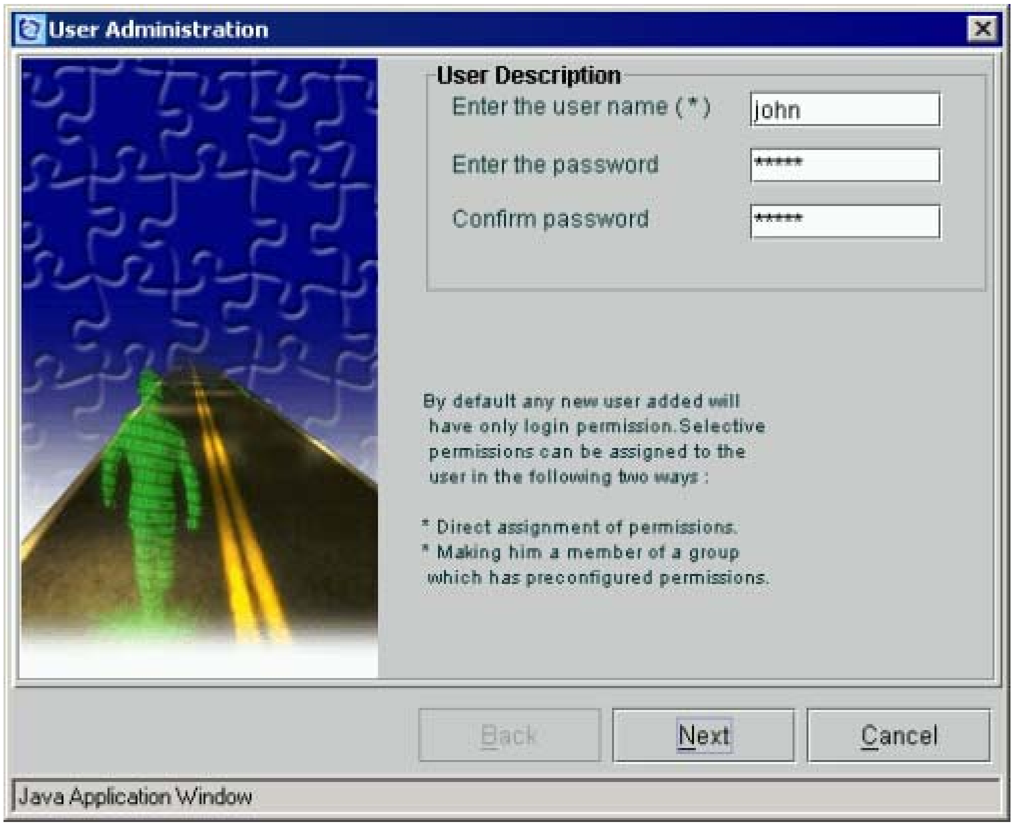
OR

Click the Add User button in the toolbar.

OR

Select the parent node and then right-click on it to select **Users-->Add User** item in the left-hand navigation pane (Integrated EMS tree).

The User Administration wizard opens, as shown in the following figure.



User Description

Enter the user name (*) john

Enter the password ******

Confirm password ******

By default any new user added will have only login permission.Selective permissions can be assigned to the user in the following two ways :

* Direct assignment of permissions.
* Making him a member of a group which has preconfigured permissions.

3 Type the user name, password and, confirmation password in the respective User Description fields. If the password is not provided, a dialog prompts the message indicating to enter a password.

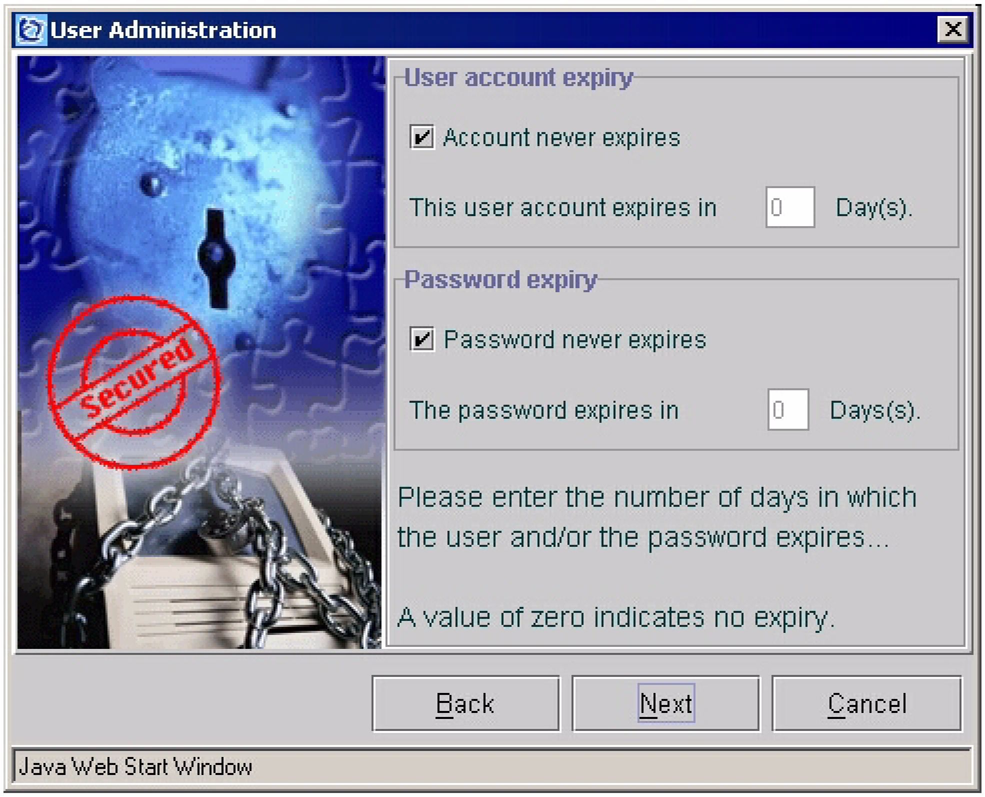
Note 1: The password restrictions described below must be followed when setting or changing a user password through any security administration system integrated with the Integrated EMS Security Server, including the Integrated EMS itself.The tools described in this section do not enforce these password restrictions when a password is set or changed. However subsequent user logins using that password results in authentication failures.

- the user name cannot be longer than 8 characters.
- passwords must be two characters or more in length.
- passwords cannot be the same as a user's name, user ID, or any other attribute stored in uid, cn, sn, giveName, ou, or mail attributes of the user'd directory entry, by default uid=<userid>, cn="", sn=Mowat, givenName=Farley, ou=People, o=<domain>.

- passwords when changed cannot be the same as any of the last six passwords.
- passwords expire after 2592000 seconds (30 days).
- use of the incorrect password can result in lockout for 120 seconds after 3 consecutive unsuccessful attempts to login.
- cannot change passwords more often than once in every 259200 seconds (3 days).

Note 2: By default, new users have only login permission. You can provide access to various modules either by making them members of pre-configured groups, or by assigning them directly to the required modules.

4 Click the **Next** button.



User Administration

User account expiry

☑ Account never expires

This user account expires in 0 Day(s).

Password expiry

☑ Password never expires

The password expires in 0 Days(s).

Please enter the number of days in which the user and/or the password expires...

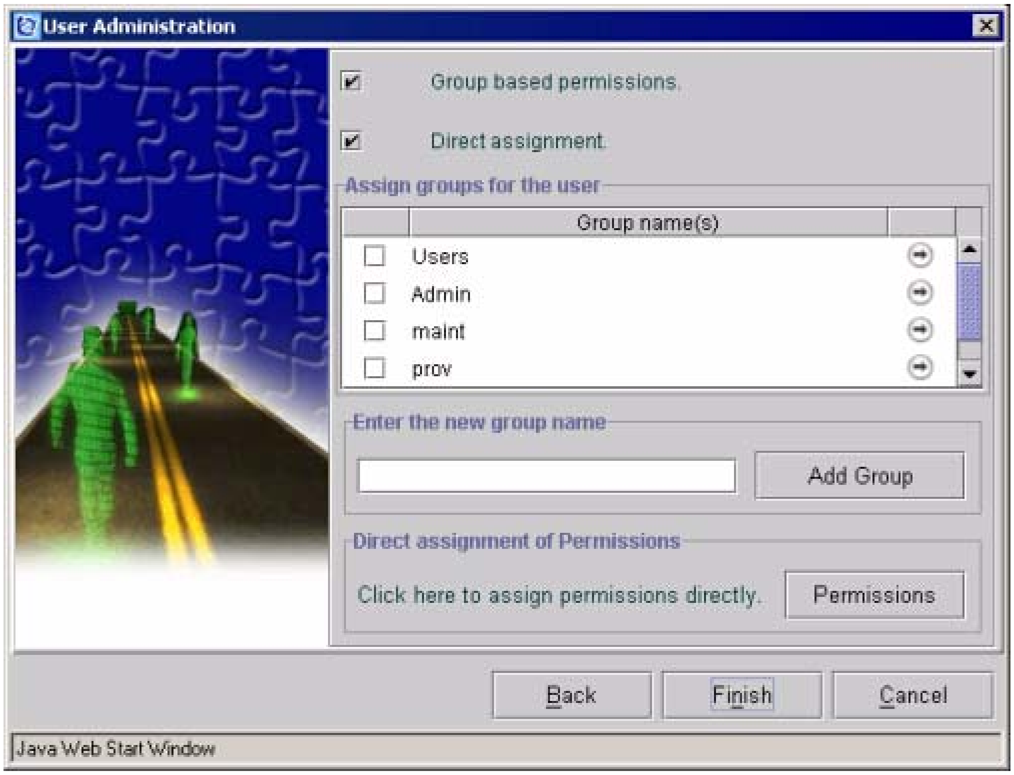
A value of zero indicates no expiry.

By default, the **Account never expires** box is checked. To provide access to the Integrated EMS Server for a particular period, uncheck the **Account never expires box** and type the required number of days in the **This user account expires in** field. **The user account** is then disabled after the specified number of days.

Similarly, by default, the **Password never expires** box is checked. To provide password expiry after a particular period, uncheck the **Password never expires** box and type the required number of days in the **This password expires** in field. The password expires after the specified number of days.

5 Click the **Next** button.

The User Administration permission assignment window opens, as shown in the following figure.



User Administration

☑ Group based permissions.

☑ Direct assignment.

Assign groups for the user

	Group name(s)	
□	Users	➡
□	Admin	➡
□	maint	➡
□	prov	➡

Enter the new group name

Direct assignment of Permissions

Click here to assign permissions directly.

6 Select the **Group based permissions** check box if you want to associate the user to an existing group.

a Select the group listed in the **Assign group for the user** table by checking the corresponding check box.

> ***Note:*** The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created at the SSPFS/Solaris level.

b If you want to add a new group to associate the user, then enter the group name and click the **Add Group** button.

Note: The group name cannot be longer than 8 characters.

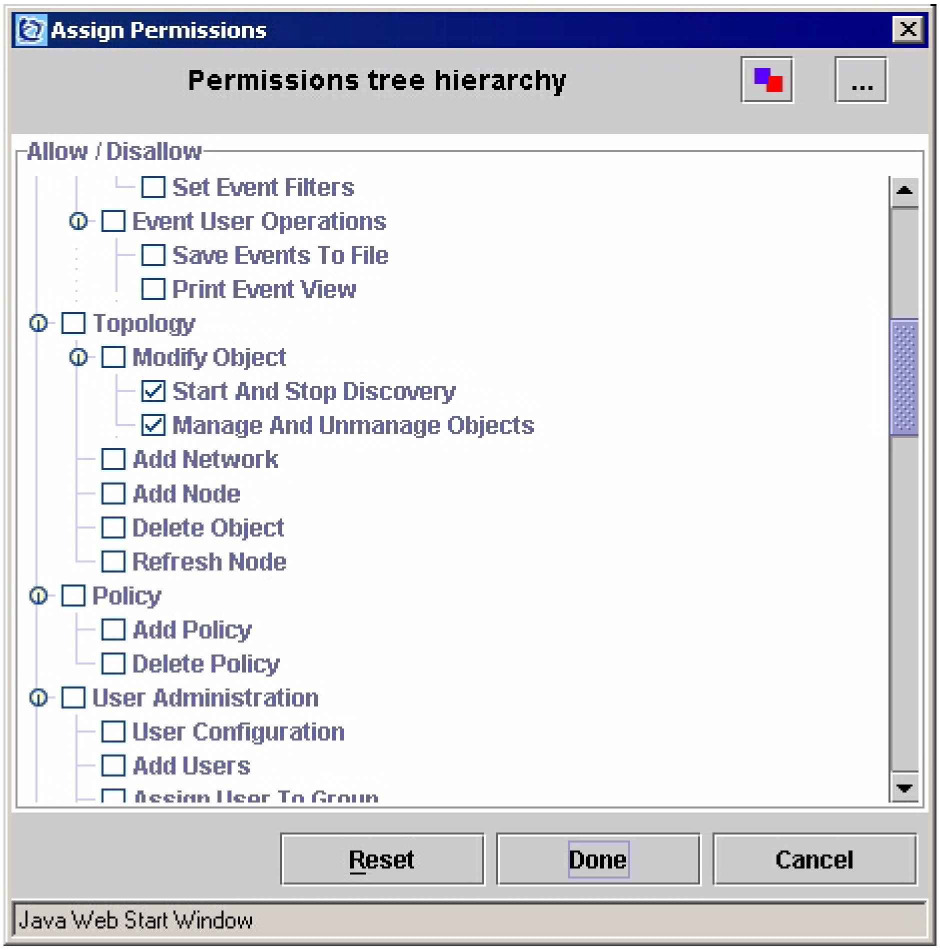
c The **Assign Permissions** dialog (refer the following figure) is displayed in which you need to associate the operations for the new group.

7 Select the **Direct assignment** check box if you are not associating the new user with any group but assigning the authorized operations directly.

The operations assigned to the user are specific to that user only.

8 Click the **Permissions** button.

The **Assign Permissions** dialog opens, as shown in the following figure.



- □ Set Event Filters
- □ Event User Operations
  - □ Save Events To File
  - □ Print Event View
- □ Topology
  - □ Modify Object
    - ☑ Start And Stop Discovery
    - ☑ Manage And Unmanage Objects
  - □ Add Network
  - □ Add Node
  - □ Delete Object
  - □ Refresh Node
- □ Policy
  - □ Add Policy
  - □ Delete Policy
- □ User Administration
  - □ User Configuration
  - □ Add Users
  - □ Assign User To Group

9 Select the required operations (Allow, Disallow, or not selected).

10 Click the **Done** button to execute the selected operations.

11 Click the **Back** button to make any changes in previous screens.

12 Click the **Finish** button.

The system creates a new user with the specified permissions. The Security Administration tool displays the new user in the left-hand navigation pane (Integrated EMS tree) under the parent node Users.

Note 1: When a user is added to the Integrated EMS, a user account is added with same user name in UNIX (SSPFS shell). The user ID is autogenerated when the user account is added. This user ID is required when setting up platform access.

Note 2: To add locally-managed users refer to the "Setting up users on a Sun server” in the ATM/IP Solution-level Security and Administration, NN10402-600.

Configuring user settings

The Security Administration tool allows the Integrated EMS administrator to configure the user settings as required. The User Settings tasks are following:

- Listing all users
- Associating user with groups
- Setting an user profile
- Changing user password
- Assigning operations to users
- Viewing, saving and clearing audit trails
- Deleting Users
- Adding new groups

Listing all users

For performing user-oriented tasks, the Integrated EMS administrator must have a list of users.

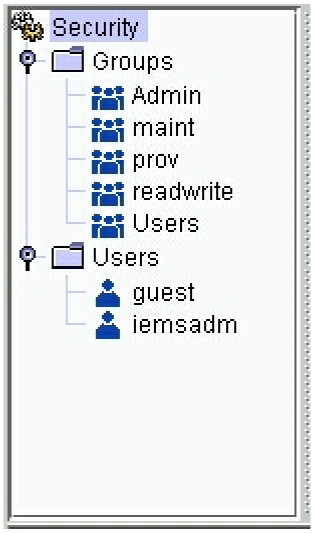
To obtain a list of all users in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Expand the **Users** node in the Security tree as shown in the following figure.

This displays the list of all users.



Associating user with groups

Integrated EMS administrator can provide group-based authorization, to assign users to groups which have configured levels of authorization.

To associate a user with an existing group in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

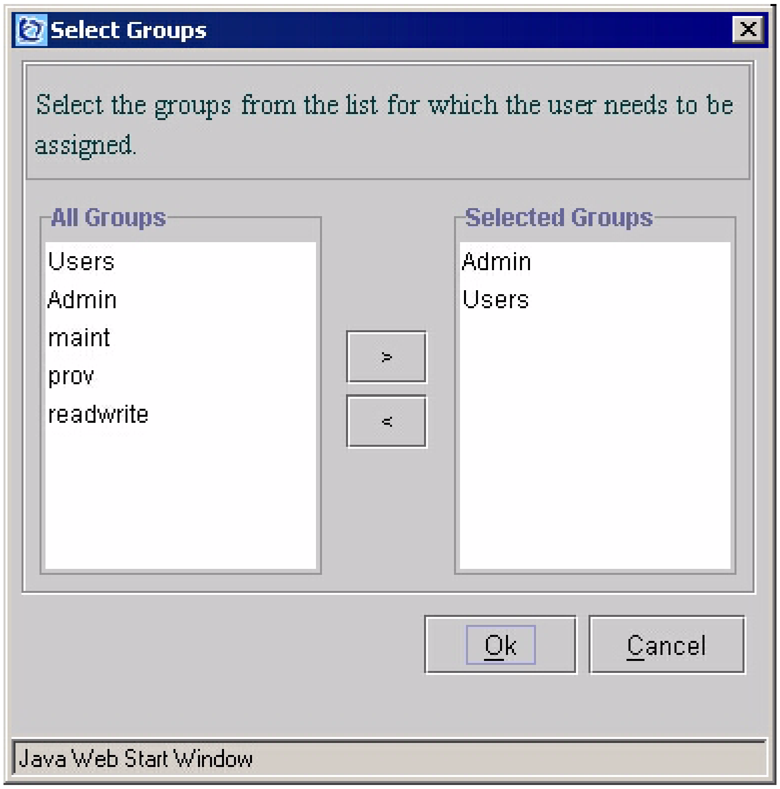
1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required user from the Security tree in the left-hand navigation pane.

3 Click the **Member Of tab** in the right-hand panel.

4 Click the **Setting Groups** button.

The Select Groups window opens as shown in the following figure. This allows you to associate the user with any of the existing groups or to remove the user from an already associated group:



Select the groups from the list for which the user needs to be assigned.

All Groups: Users, Admin, maint, prov, readwrite

Selected Groups: Admin, Users

The left-hand side of the window (All Groups) displays, all the existing groups and the right-hand side (Selected Groups) displays the, group names with which the user is already associated.

5 Select the required group from the All Groups list and click the **>** (Add) button.

The system displays the required group in the Selected Groups list and associates the user with this group. To remove the user from the already associated group, select the group from the Selected Groups list and click the < (Remove) button.

6 Click the **OK** button to update the User and Group details in Integrated EMS Server.

Viewing, saving and clearing audit trails

Integrated EMS administrator must to audit the user operations regularly to check their status, that is, whether or not operations carried out by users are successful.

Viewing audit trails

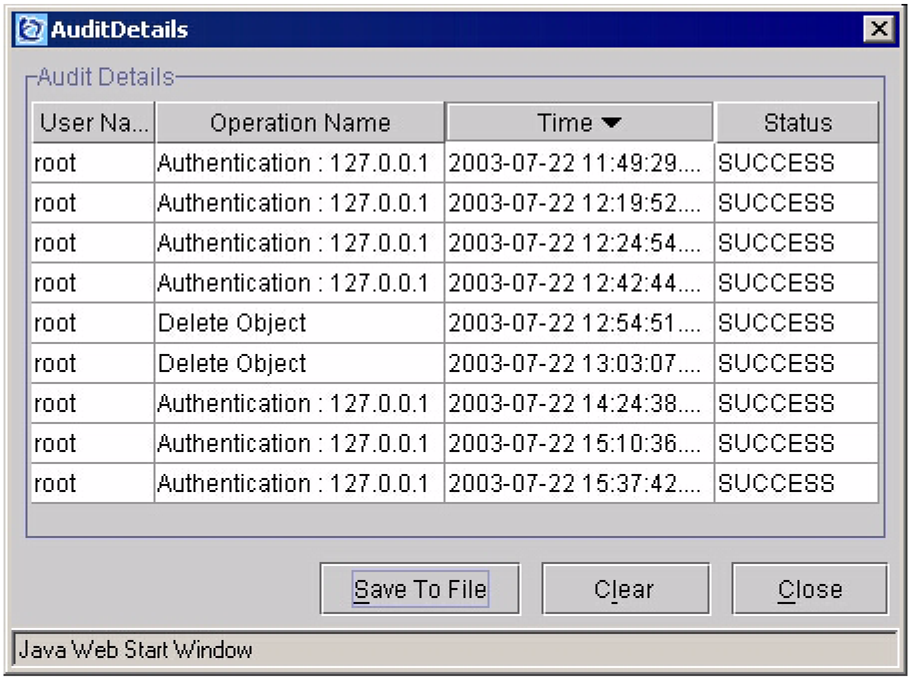
To view the audit trails of all the users in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the **View-->Audit Trails** menu command.

This opens the Audit Details window as shown in the following figure.



User Na...	Operation Name	Time ▼	Status
root	Authentication : 127.0.0.1	2003-07-22 11:49:29....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 12:19:52....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 12:24:54....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 12:42:44....	SUCCESS
root	Delete Object	2003-07-22 12:54:51....	SUCCESS
root	Delete Object	2003-07-22 13:03:07....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 14:24:38....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 15:10:36....	SUCCESS
root	Authentication : 127.0.0.1	2003-07-22 15:37:42....	SUCCESS

The table shows the audit trails for all users, with details of the operations performed, date and time, and status (SUCCESS or FAILURE). For an authentication operation, the table also includes the host IP address.

3 Click the **Close** button to close the window.

Saving audit trails

Audit trails can be stored in the Integrated EMS Server with a specified file name.

To save the audit trails of all users in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the “Starting the Security Administration Tool”)
2. Select the **View-->Audit Trails** menu command.

   This opens the Audit Details window.
3. Click the **Save To File** button.

   This opens the **Save** dialog.
4. Enter the file name and click the **Save** button to save the file.
5. Click the **Close** button to close the window.

   This file can be used for future reference to identify any access violation. The file with the specified name is saved under the <IEMS Home> directory.

Clearing Audit Trails

Audit trails can be cleared from the Integrated EMS Server. This must be done regularly, for example, after saving the details to a file.

To clear the audit trails of all users in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the “Starting the Security Administration Tool”)
2. Select the **View-->Audit Trails** menu command.

   This opens the **Audit Details** window.
3. Click the **Clear** button to clear all the current audit trials from the Integrated EMS Server.
4. Click the **Close** button to close the window.

Setting an user profile

Integrated EMS Server administrator can change the user profile details such as user status, password, account termination, and password expiry.

To change the user profile in the Integrated EMS, follow these steps:

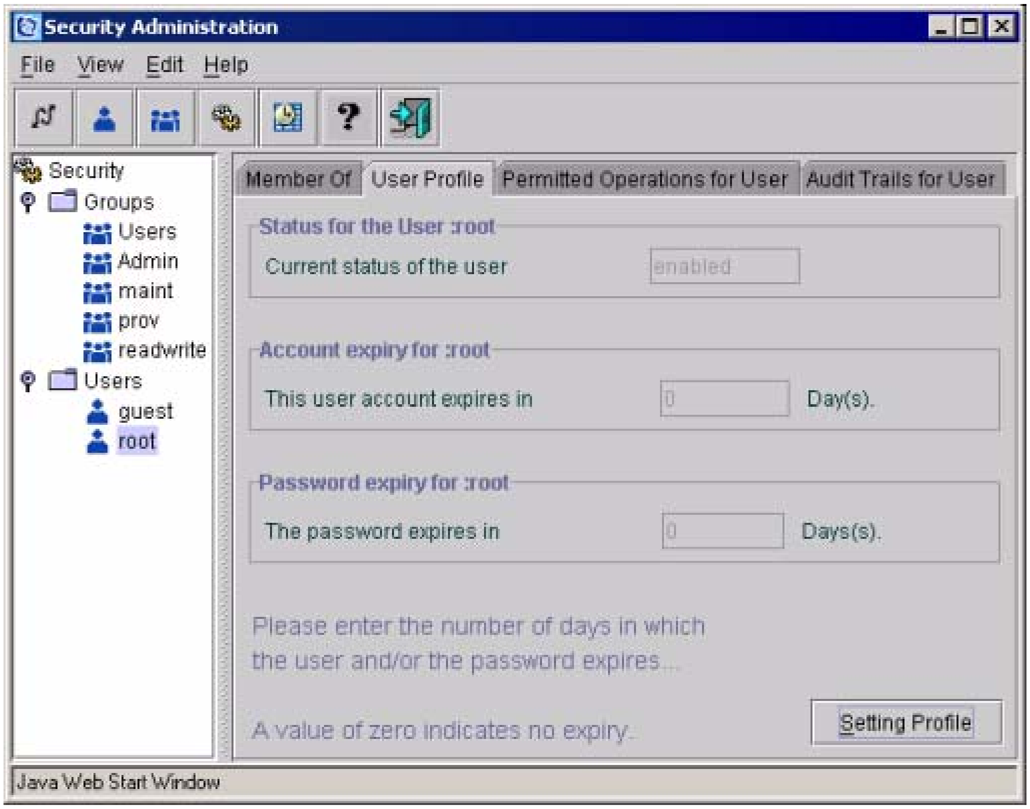
In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required user from the Security tree in the left-hand navigation pane.

3 Click the **User Profile** tab in the right-hand panel.

This displays the current user status, user account expiry, and password expiry as shown in the following figure



Status for the User :root

Current status of the user: enabled

Account expiry for :root

This user account expires in 0 Day(s).

Password expiry for :root

The password expires in 0 Days(s).

Please enter the number of days in which the user and/or the password expires...

A value of zero indicates no expiry.

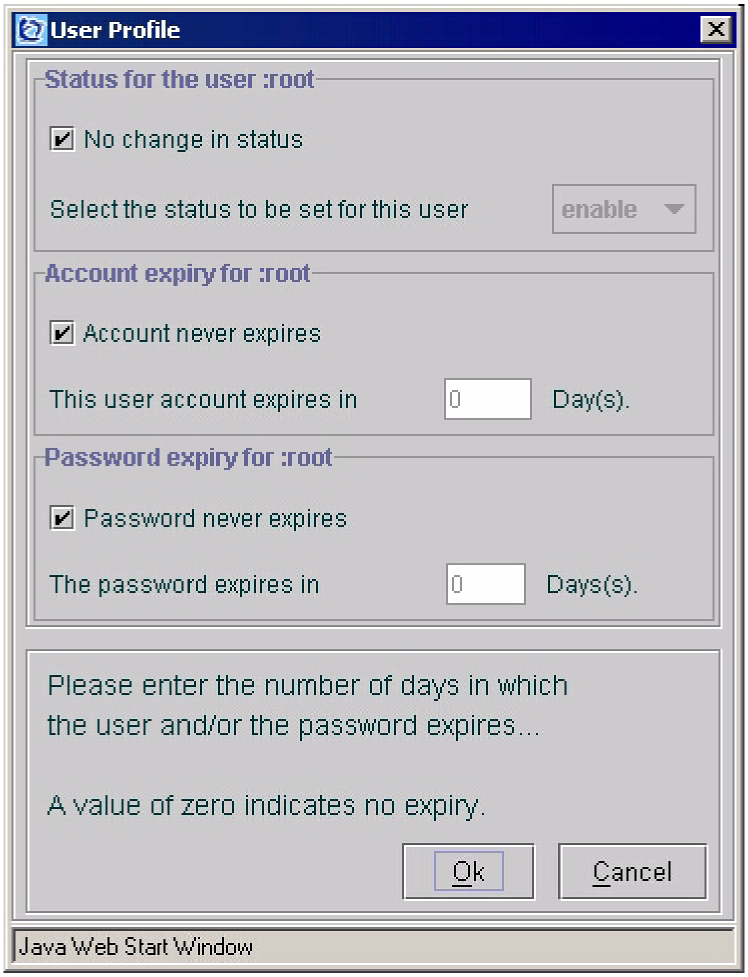
Note: By default, the user status is "enabled", but if you set the status of the newly created user to "disable" in the **Status**

for the User field, the Integrated EMS Security administration tool can take up to 24 hours to disable the command line access to the Integrated EMS server. You can disable an account immediately by setting the user’s shell to /bin/false. To set the user’s shell to /bin/false, log in to the Integrated EMS server as root and type the command,

usermod -s /bin/false <username>

4 Click the **Setting Profile** button at the bottom right-hand corner of the screen.

This opens the **User Profile** dialog, as shown in the following figure:



User Profile

Status for the user :root

☑ No change in status

Select the status to be set for this user: enable

Account expiry for :root

☑ Account never expires

This user account expires in 0 Day(s).

Password expiry for :root

☑ Password never expires

The password expires in 0 Days(s).

Please enter the number of days in which the user and/or the password expires...

A value of zero indicates no expiry.

5 Set the user status as required by selecting the **No changes in status** check box, enable or disable.

6 Set the account expiry time by unchecking the **Account never expires** check box and typing the required number of days.

The user account is disabled after the specified expiry time and the user is not allowed to connect to the Integrated EMS Server.

7 Set the Password expiry time by unchecking the **Password never expires** check box and typing the required number of days.

After the specified expiry time, the user is prompted to enter a new password.

8 Click the **OK** button to update the user profile details in Integrated EMS Server.

Changing user password

The administrator can change the user password for security reasons. The password can be changed in Security Administration GUI or with Password Configurator GUI. This section explains the procedure to change the password in these GUIs.

> ***Note:*** The password restrictions described below must be followed when setting or changing a user password through any security administration system integrated with the Integrated EMS Security Server, including the Integrated EMS itself.The tools described in this section do not enforce these password restrictions when a password is set or changed. However subsequent user logins using that password result in authentication failures.
>
> - passwords must be two characters or more in length.
> - passwords cannot be the same as a user's name, user ID, or any other attribute stored in uid, cn, sn, giveName, ou, or mail attributes of the user'd directory entry, by default uid=<userid>, cn=”cn=””, sn=Mowat, givenName=Farley, ou=People, o=<domain>.
> - passwords when changed cannot be the same as any of the last six passwords.
> - passwords expire after 2592000 seconds (30 days).
> - use of the incorrect password can result in lockout for 120 seconds after 3 consecutive unsuccessful attempts to login.
> - cannot change passwords more often than once in every 259200 seconds (3 days).

Changing user password in Security Administration GUI

To change the user password in the Security Administration tool of Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).
2. Select the required user from the Security tree in the left-hand navigation pane.
3. Select the **Edit-->Change Password** menu command to launch the Change Password dialog.

4 Type the new password and confirmation password.

Note: If the password is not provided, a dialog prompts the message indicating to enter a password.

If the password is same as user name, a dialog prompts the message indicating that password cannot be same as user name and enter different password.

5 Click the **OK** button to update the password in the Integrated EMS Server.

Changing user password with Password Configurator GUI

The user can change the user password using the **Password Configurator** dialog in the Integrated EMS Client user interface. To change the password with the Password Configurator GUI for the user currently logged in, follow these steps:

At the Integrated EMS workstation

1 Refer to the “Launching Integrated EMS Java Web Start Client” of the *Integrated EMS Basics*, NN10329-111 to launch the Integrated EMS Client.

2 Select the **Tools-->Change Password** menu command to launch the Password Configurator dialog.

3 Type the new password and confirmation password.

Note: If the password is not provided, a dialog prompts the message indicating to enter a password.

If the password is same as user name, a dialog prompts the message indicating that password cannot be same as user name and enter different password.

4 Type the duration after which the password must expire in the **Password Expiry duration** field.

5 Click the **OK** button to update the password in the Integrated EMS Server.

Assigning operations to users

Integrated EMS administrator can assign various operations to a user. These can be additional operations, which are not authorized via the user’s group.

To assign operations to a user in the Integrated EMS, follow these steps:

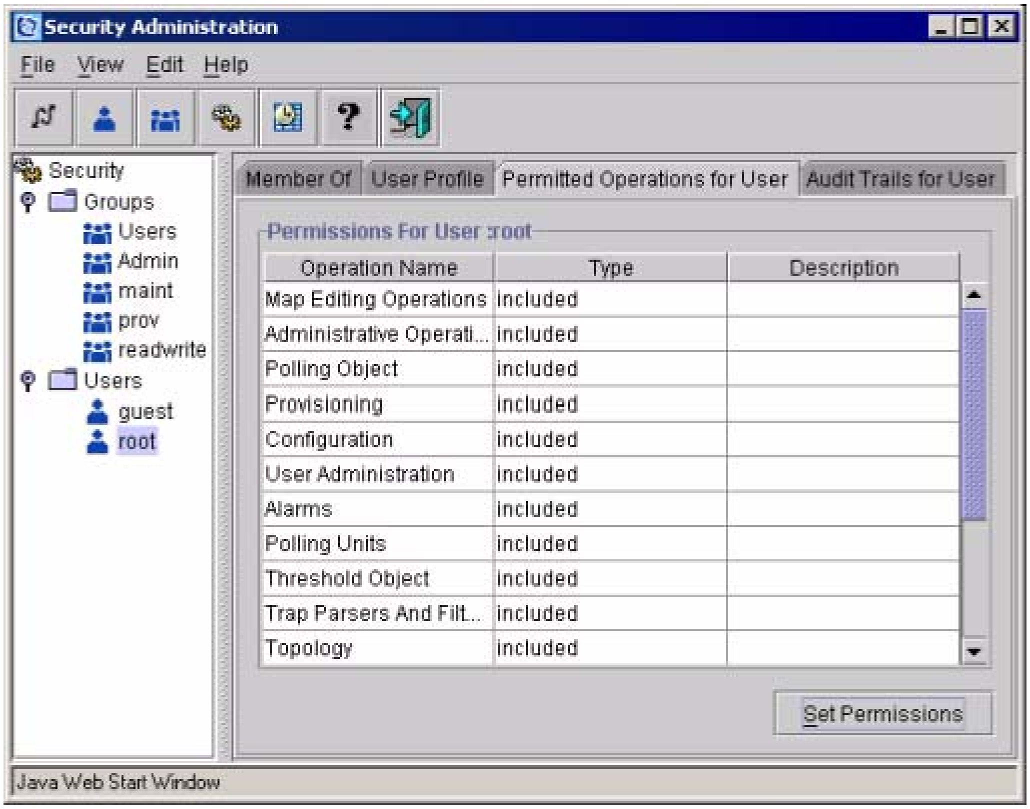
In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Select the required user from the Security tree in the left-hand navigation pane.

3 Click the **Permitted Operations for User** tab in the right-hand panel.

This displays the operations currently assigned to the user, as shown in the following figure.



Permissions For User :root

Operation Name	Type	Description
Map Editing Operations	included	
Administrative Operati...	included	
Polling Object	included	
Provisioning	included	
Configuration	included	
User Administration	included	
Alarms	included	
Polling Units	included	
Threshold Object	included	
Trap Parsers And Filt...	included	
Topology	included	

4 Click the **Set Permissions** button at the bottom right-hand corner of the screen.

This opens the Assign Permissions dialog.

The Permissions tree displays all the operations available. The check boxes show the operations currently assigned to the user (either directly assigned or through groups).

> ***Note:*** Group-based permissions co-exist with direct assignment. If you provide group-based permissions and direct assignments, the user is authorized to carry out all the group-based and directly assigned operations.

5 Use the check boxes in the tree to select the required operations for the user.

6 Click the **Done** button to update the operation details in the Integrated EMS Server.

> ***Note:*** To change the user's group-based permissions, select the group to which the user belongs, then click the **Permitted Operations For Group tab**. Follow the step 4 to step 6 of the above procedure.

Deleting Users

Integrated EMS administrator must update the user accounts regularly and delete the accounts of users who are not authorized to access the Integrated EMS. Deleting user accounts involves following steps:

1. Disabling the user account
2. Deleting the user account on an SSPFS Security Client
3. Deleting the user account in Security Administration tool

Disabling the user account

To disable a centrally-managed user in the Integrated EMS Server shell, follow these steps:

In the Integrated EMS workstation

1 In a web browser launch the Token Administration tool and login to the tool:

```
http://<hostname>:8080/tokenadmin/
```

where <hostname> is the host name of the Integrated EMS Server.

2 In the Token Administration tool, select all the single sign-on tokens associated with the user account, and delete the tokens.

3 Disable the user platform access by setting the user shell access to false as in the following sub-steps.

a Login to the Integrated EMS Server as root.

b Run the following usermod command to disable shell access

```
# usermod -s /bin/false <username>
```

4 If the Integrated EMS Server is in HA configuration, then login to the inactive cluster node and repeat step 3.

Deleting the user account on an SSPFS Security Client

To delete the centralized user account on an SSPFS Security Client, follow these steps:

At the SSPFS client machine

1 Ensure the user is completely logged out of the SSSPFS client (all user sessions closed).

2 Login to the SSPFS client machine as the root user.

3 Delete the user home directory.

4 At the Unix prompt, type the following command and press "Enter" key.

```
userdel <username>
```

5 If the Integrated EMS server is in HA configuration, then perform the steps step 1 to step 4 on the active and inactive cluster node.

Deleting the user account in Security Administration tool

To delete a centrally-managed user in the Integrated EMS, follow these steps:

At the Integrated EMS workstation

1 Launch the Security Administration tool in Integrated EMS Client (refer to the “Starting the Security Administration tool”).

2 Select the required user from the Security tree in the left-hand navigation pane.

3 Select the **Edit-->Delete** menu command.

4 The system prompts for confirmation and you must click “Yes” in the confirmation dialog box to delete the user account.

Note: To delete locally-managed users refer to “Deleting a user from a Sun server” in the ATM/IP Solution-level Security and Administration, NN10402-600

Adding new groups

Integrated EMS Server allows group-based authorization.Different types of users are organized into groups, for example Users, Admin, maint, prov, readwrite. The group profile specifies a set of common operations that can be performed by the users in that group. Group-based authorization saves the Integrated EMS administrator's time in creating and managing users and their associated operations in Integrated EMS.

To add a new group in Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the **File-->New-->AddGroup** menu command.

OR

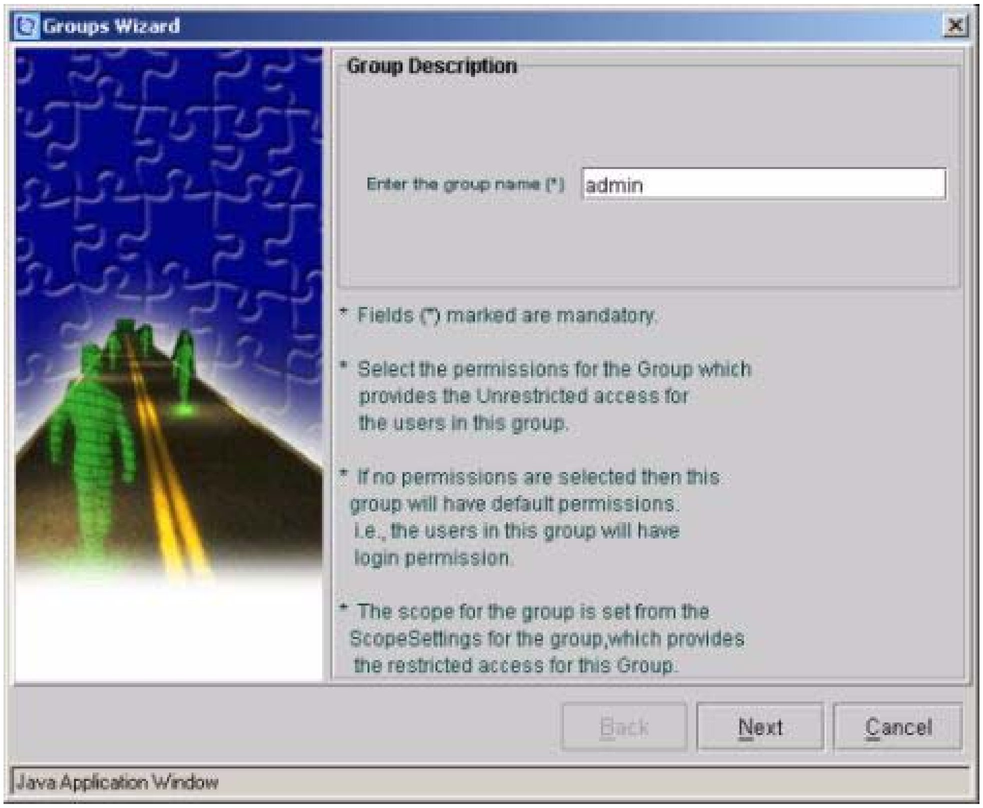
Click **Add Group** button in toolbar.

OR

Select the **Groups** node in the Security tree in the left-hand navigation pane and right click on it to select the **Add Group** menu item.

This opens **Groups Wizard** window as shown below:

Groups Wizard window



Enter the group name (*) admin

* Fields (*) marked are mandatory.

* Select the permissions for the Group which provides the Unrestricted access for the users in this group.

* If no permissions are selected then this group will have default permissions. i.e., the users in this group will have login permission.

* The scope for the group is set from the ScopeSettings for the group,which provides the restricted access for this Group.

3 Type the group name and click the **Next** button.This opens the Permissions window for the group.

Note: The group name cannot be longer than 8 characters.

4 Use the check boxes in the tree to select the required operations:

- Check the boxes to include those operations.
- Deselect the check boxes (x) to exclude operations.
- Leave the check boxes empty for operations not counted as authorized operations (such operations inherit their immediate parent operation's permission).

5 Click the **Finish** button.

The system creates a new group with the specified permissions. The Security Administration tool displays the new group in the left-hand navigation pane (Security tree) under the parent node Group.

Configuring scope and group settings

Authorized scopes (or authorized views) are independent entities, which store authorization information. The scopes are associated with the actual operations of the group leading to detailed authorization for the user. Scopes consist of a set of properties and are applicable only when those properties are true.

For example, if you specify a property as network=192.168.4.32 (name=network and value=192.168.4.32,), the scope of that associated operation is applicable only to that network. The scopes associated with the respective operations are grouped together under the groups and then allocated to the users. Integrated EMS administrator can perform the following scope configuration tasks:

- Adding a scope
- Changing a scope
- Deleting a scope

Integrated EMS administrator can perform the following group configuration tasks:

- Assigning a user to a group
- Assigning operations to a group

Adding a scope

This section describes the procedure for adding a new scope to an existing group. For a description of scope, refer to the “Configuring scope and group settings“section.

To add a scope to the Integrated EMS, follow these steps:

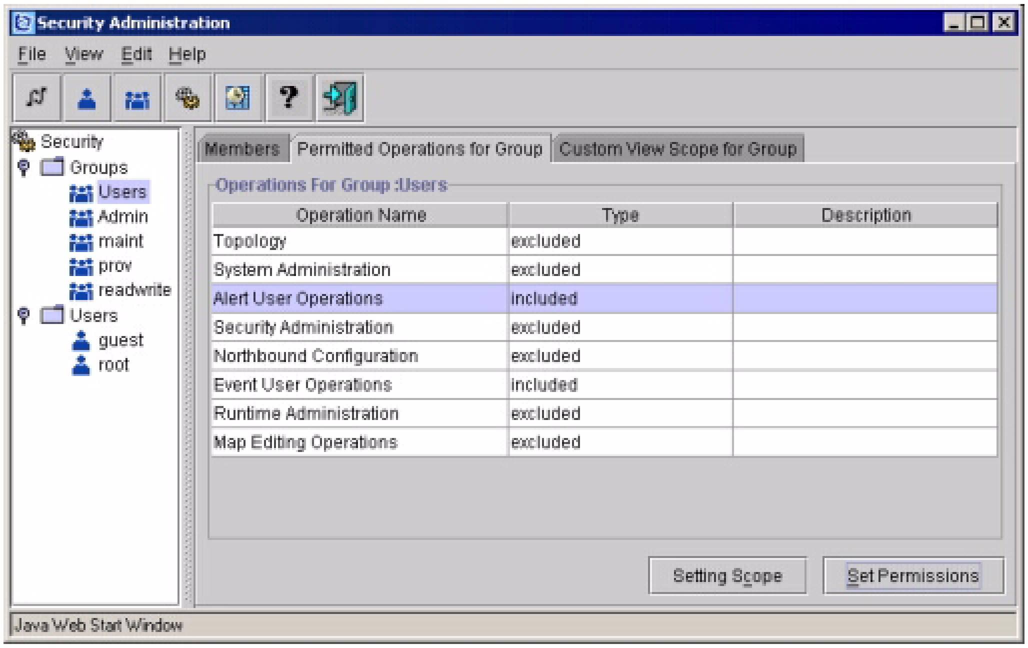
In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Select the required group (for which you want to set a scope) under the Groups node in the Security tree.

3 Select the **Permitted Operations for Group** tab from the right-hand panel.

4 Select the operation for which you want to set a scope, as shown in the following figure.



Operations For Group :Users

Operation Name	Type	Description
Topology	excluded	
System Administration	excluded	
Alert User Operations	included	
Security Administration	excluded	
Northbound Configuration	excluded	
Event User Operations	included	
Runtime Administration	excluded	
Map Editing Operations	excluded	

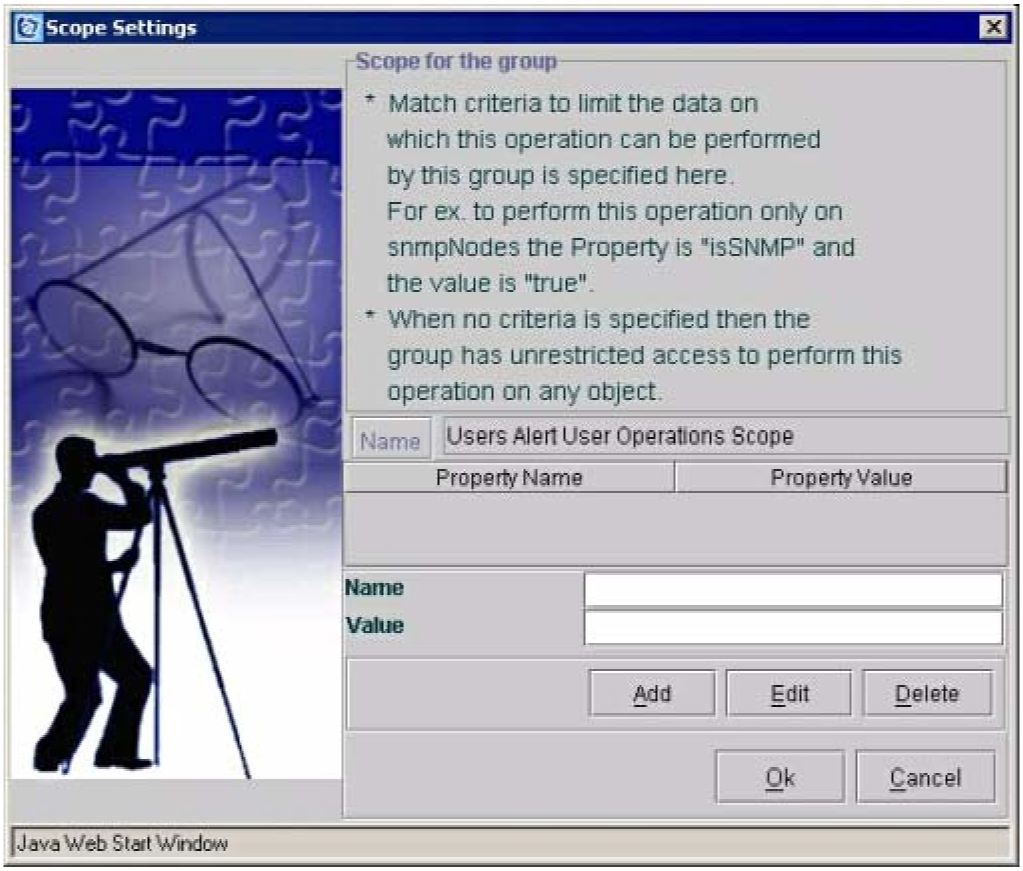
The meaning of the Type values is as follows:

- included - the operation is an authorized operation of the view
- excluded - the operation is not an authorized operation of the view
- don’t care - the authorization of the operation is not specified; the value is taken to be the same as for its parent operation

Note: The Setting Scope button is enabled only if the Type value for that operation is “included”; you cannot set a scope if the Type value is “excluded” or “don’t care”.

5 Click the **Setting Scope** button.

This opens the Scope Settings dialog, as shown in the following figure.



* Match criteria to limit the data on which this operation can be performed by this group is specified here. For ex. to perform this operation only on snmpNodes the Property is "isSNMP" and the value is "true".

* When no criteria is specified then the group has unrestricted access to perform this operation on any object.

Name: Users Alert User Operations Scope

Property Name	Property Value

6 Type the property name and property value for the new scope in the **Name** and **Value** fields respectively.

7 Click the **Add** button to add the new scope.

8 Click the **OK** button to save the changes in the Integrated EMS Server.

Changing a scope

You can modify the existing scope for the group. For a description of scope, refer to the “Configuring scope and group settings“section.

To change existing scope in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Select the required group (for which you want to change the scope) under the Groups node in the Security tree.

3 Select the **Permitted Operations for Group** tab in the right-hand panel.

4 Select the operation for which you want to change the scope.

5 Click the **Setting Scope** button.

This opens the Scope Settings dialog.

6 Select the scope to be changed from the Property or Value table.

7 Type the name and value, and click the **Edit** button to update the scope.

8 Click the **OK** button to save the changes in the Integrated EMS Server.

Deleting a scope

You can delete an existing scope for the group. For a description of scope, refer to the “Configuring scope and group settings“section.

To delete an existing scope in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Select the required group (for which you want to delete the scope) under the Groups node in the Security tree.

3 Select the **Permitted Operations for Group** tab in the right-hand panel.

4 Select the operation for which you want to delete the scope.

5 Click the **Setting Scope** button.

The Scope Settings dialog opens.

6 Select the scope to be deleted from the Property or Value table.

7 Click the **Delete** button to delete the selected scope.

8 Click the **OK** button to save the changes in the Integrated EMS Server.

> ***Note:*** Scopes can be configured to operations of groups with properties. Administrators can add a list of scope to a single operation or more of the groups and then assign the group to the users. Thus properties are added for detailed authorization.

Assigning a user to a group

Integrated EMS administrator can assign users to a selected group to restrict the set of users performing the operations that are permitted for that group.

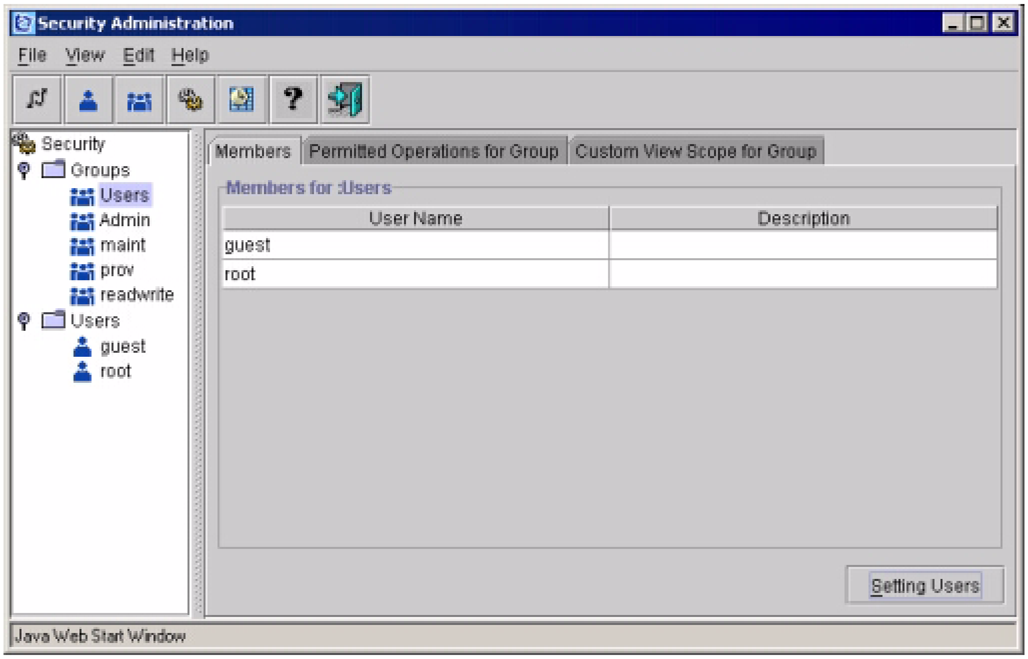
To assign a user to the group in the Integrated EMS, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required group in the left-hand side navigation pane.

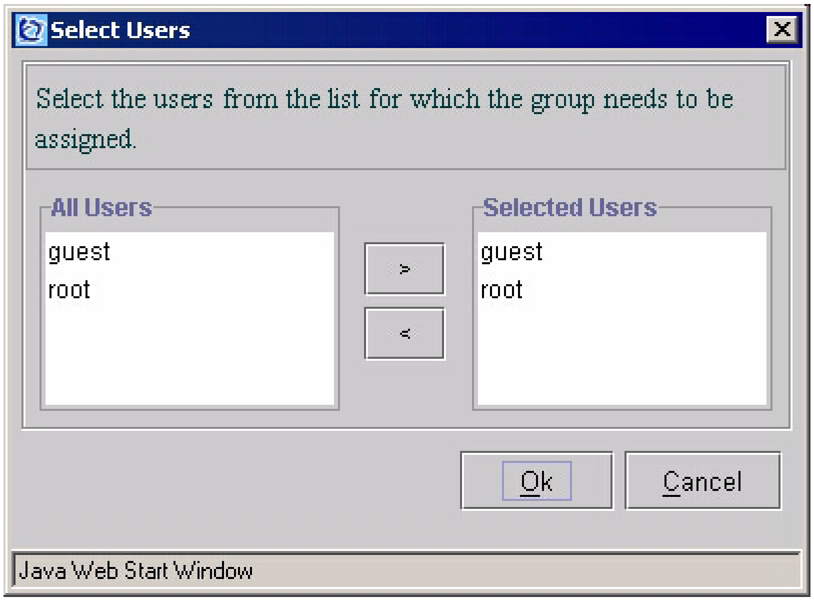
3 Click the **Members tab** in the right-hand panel, as shown in the following figure.



User Name	Description
guest	
root	

4 Click the **Setting Users** button.

The **Select Users** dialog opens, as shown in the following figure.



Select Users

Select the users from the list for which the group needs to be assigned.

The left-hand side of the window (All Users) displays all the user names, and the right-hand side (Selected Users) displays the selected users for that particular group.

5 Select the required user from the All Users list and click the > (Add) button to assign the user to the group.

> ***Note:*** The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created at the SSPFS/Solaris level.

6 Click the **OK** button to update the changes in the Integrated EMS Server.

Assigning operations to a group

The administrator can assign the operations that a group can perform.

To assign an operation to a group, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required group in the left-hand navigation pane.

3 Click the **Permitted Operations for Group** tab in the right-hand panel.

This displays all the operations included or excluded for the selected group.

4 Click the **Set Permissions** button.

This opens the **Assign Permissions** dialog.

5 Select the check boxes against each operation to allow or not allow the required operations.

6 Click the **Done** button to update the operation details in the Integrated EMS Server.

The list of operations that are privileged for the "Admin" group are:

S. No:	Operation
1	Map Editing Operations
2	Administrative Operations
3	Polling Object
4	Provisioning
5	Configuration
6	User Administration
7	Alerts
8	Polling Units
9	Trap Parsers and Filters

S. No:	Operation
10	Threshold Object
11	Topology
12	Job
13	Events
14	Poll Filters
15	Event Filters and Parsers

User mapping in security administration

Integrated EMS authorization system allows for the assignment of users to groups, with specific sets of tasks defined for each group. This section lists the various groups with the permitted tasks for the users in that group.

Administration: The users in this group are permitted to do following tasks:

- Re configuring the system.
- Accessing all functions.
- Setting up of fundamental configuration.
- Commissioning the (add, delete or rename) base frames or systems (SAM21 frames, Call servers, and large gateways)
- Running service impacting diagnostics.

Users:The users in this group are permitted to view configuration and status, but cannot make changes in configurations or status.

Read/Write: The users in this group are permitted to do following tasks:

- Viewing the status and configuration
- Changing the status and configuration
- Reconfiguring the elements such as GWC, cards, shelves

Provisioning: The users in this group are permitted to do following tasks:

- Viewing status and configuration
- Changing provisioning data; cannot change mtc state or do base component configuration

Maintenance: The users in this group are permitted to do following tasks:

- Viewing the configuration and the status
- Changing the status
- Running the service-impacting diagnostics

The following table shows the groups with their target network components.

Mapping of User Groups for each Role in Integrated EMS Modules

	Target				
Role	**Line**	**Trunk**	**MG (Gateways)**	**MGC (Call Servers and Central Components)**	**EMS/EML**
Administration	lnadm	trkadm	mgadm	mgcadm	emsadm
Users	lnro	trkro	mgro	mgcro	emsro
Read Write	lnrw	trkrw	mgrw	mgcrw	emsrw
Provisioning	lnsprov	trksprov	mgsprov	mgcsprov	emssprov
Maintenance	lnmntc	trkmntc	mgmntc	mgcmntc	emsmntc

The following table shows the mapping of default users with user groups.

User Mapping with Default Users

Default User Name	Member of Group
guest	Users
iemsadm	Admin and Users

Using custom view scope

A custom view scope for a group filters Integrated EMS objects so that users can view only the data on which they are authorized to perform operations.

Integrated EMS administrator can perform the following custom view scope tasks for a group:

- Adding an authorized custom view scope
- Setting an authorized custom view scope
- Setting custom view scope properties
- Deleting an authorized custom view scope

Adding an authorized custom view scope

Integrated EMS administrator can add the authorized Custom View Scope to the group. This section describes the procedure to add the authorized custom view scope to the group.

To add an authorized custom view scope to the group, follow these steps:

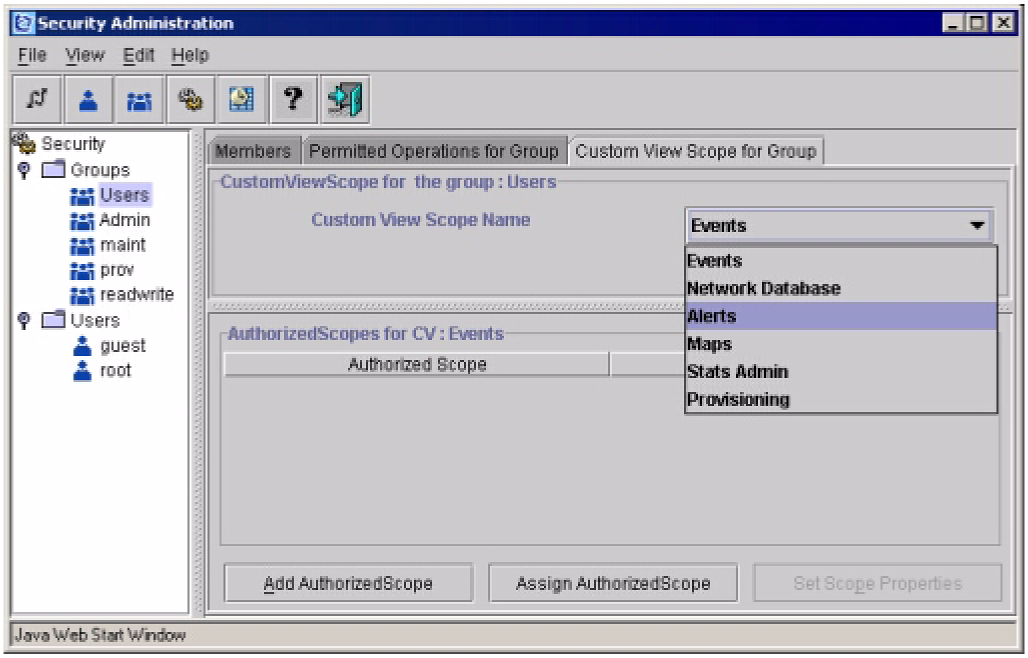
In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required group under the Groups node in the Security tree.

3 Click the **Custom View Scope for Group** tab in the right-hand panel.

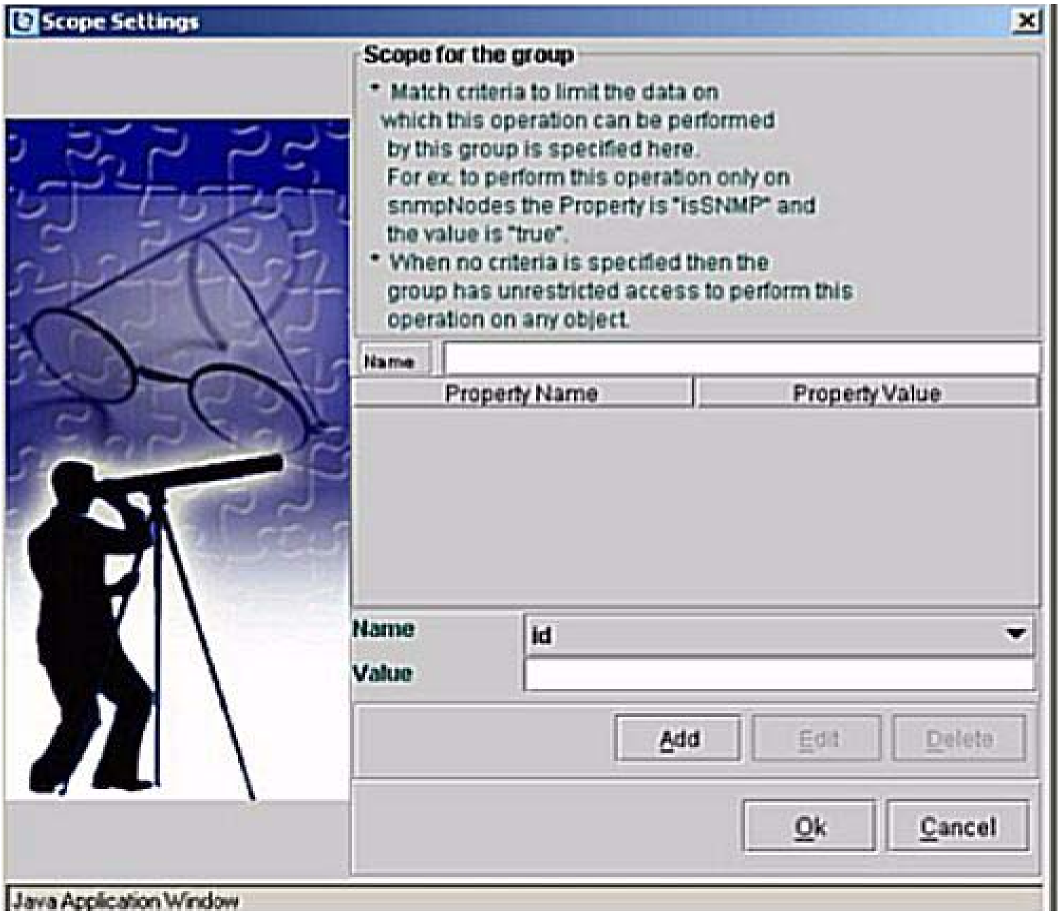
The "Custom View Scope for the groups" window opens, as shown in the following figure.



4 Select the required custom view scope name from the drop-down menu.

5 Click the **Add AuthorizedScope** button. For example, select the Events Custom View Scope and click *Add Authorized Scope*

button. The Scope Settings dialog opens, as shown in the following figure.



Scope Settings

Scope for the group

- Match criteria to limit the data on which this operation can be performed by this group is specified here. For ex. to perform this operation only on snmpNodes the Property is "isSNMP" and the value is "true".
- When no criteria is specified then the group has unrestricted access to perform this operation on any object.

Name

Property Name	Property Value

Name: id

Value:

6 Specify a name for the created custom view in the **Name** textfield. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes.

Example
If an Event Custom View scope is selected for adding, then the property name drop down box displays properties of the event object such as severity, type, name and so on.

Similarly, for Topology, Alarm, and Configured Collection sections, properties of managed object (MO), alarm object and polling object are listed, respectively in the property name drop down box.

7 Enter the value for the property in **Value** field. To identify more than one property value, separate each value according to the appropriate operator in the following Value Operators table:

Value Operator	Description
* (Asterisks)	Use an asterisk to filter on a match of zero or more characters. Example: To view all objects starting with the name test, set the property key as name and the value as test*.
! (Exclamation Mark	Use an exclamation mark to filter the search using the NOT operator. Example: To view all objects whose names do not start with test, set the property key as “name” and value as “!test*”.
, (Comma)	Use a comma to filter objects where a single property key has different values. Example: To view all objects with names starting with abc or xyz, set the property key as name and value as abc*,xyz*.
&& (Ampersand	Use an ampersand to filter objects where a single value needs to be matched with many patterns. Example: To view all objects with names starting with abc and ending with xyz, set the property key as name and value as abc*&&*xyz

Value Operator	Description
\ (Back Slash)	Use a back slash to filter objects when the name of the object itself contains a comma. This character is called an escape sequence because it avoids searching for objects, as if they had two different names. Example: To view an object with name a,b, set the property key as name and the value as a\,b.
<between> value1 and value2	Use greater than and less than signs to filter objects with numeric values within a specific range. Example: If object names with a poll interval value ranging between or including 300 and 305 are required, set the property key as pollinterval and value as <300 and 305>. Note that the first number is smaller than the second number. Only the values in between the given values, including the limits, are matched.

8 Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

9 Click the **OK** button to update the scope details in the Integrated EMS Server.

Setting an authorized custom view scope

Integrated EMS administrator can set the Authorized Scope for the selected Custom View Scope to the group.

To set Authorized Scope for the selected Custom View Scope, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

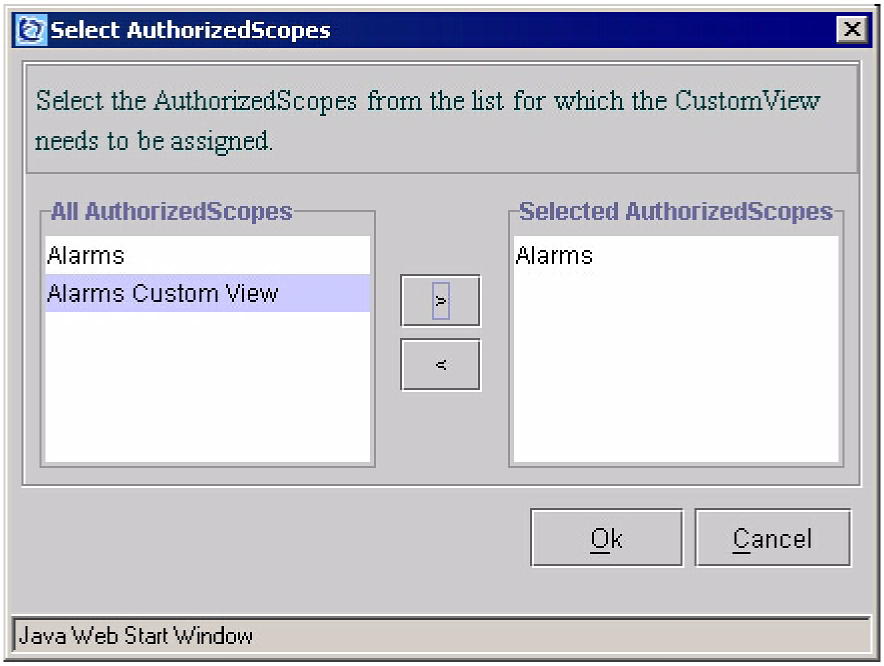
2 Select the required group under the Groups node in the Security tree.

3 Click the **Custom View Scope for Group** tab in the right-hand panel to display all the custom view scopes for the selected group.

4 Select the required Custom View Scope name from the drop-down comb menu.

5 Click the **Assign AuthorizedScopes** button.

This opens the Select AuthorizedScopes dialog, as shown in the following figure.



Select AuthorizedScopes

Select the AuthorizedScopes from the list for which the CustomView needs to be assigned.

All AuthorizedScopes: Alarms; Alarms Custom View

Selected AuthorizedScopes: Alarms

The left-hand side of the window (All AuthorizedScopes) displays all the Authorized Scopes set for the operations of the groups in the left-hand column and the right-hand column (Selected AuthorizedScopes) displays the previously set Authorized Scopes or the selected Custom View Scope name.

6 Select the required scope to be set for the Custom View in the left and click the > (Add) button. To remove the already existing Authorized Scope set for the Custom View, select the required scope in the right-hand column, and click the < (Remove) button.

7 Click the **OK** button to update the Integrated EMS Server.

Setting custom view scope properties

Integrated EMS administrator can set the properties of the Authorized Custom View Scope.

To set the properties of the Authorized Custom View Scope, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Click the **Custom View Scope for Group** tab in the right-hand panel to display all the custom view scopes for the selected group.

3 Select the required row of the Authorized Scope (of the selected Custom View Name).

This enables the Set ScopeProperties button.

4 Click the **Set ScopeProperties** button to open the Scope Settings dialog.

5 Add or change the necessary properties for the selected Authorized Scope in the Property table.

In the Scope Settings dialog, specify the set of wild card characters that are supported in Integrated EMS Server. The following table provides descriptions of the various operators that can be used to specify the scope criteria values in the Scope Settings dialog.

Description of operators used in Scope Settings dialog

Operator	
* (Asterisk)	Used to match zero or more characters. **Example** To search for all objects whose names start with the characters “test”, specify the Property Key name and the Value test*.
!(Exclamation Mark)	Used for filtering a search using the NOT operator **Example** To search for all objects whose names do not start with the characters “test”, specify the Property Key name and the Value!test*.

Description of operators used in Scope Settings dialog

Operator	
, (Comma)	Used for searching for objects where a single property key has different values. **Example** To search for all objects whose names start with the characters “abc” or “xyz”, specify the Property Key name and the Values abc*,xyz*.
&& (Ampersand)	Used for searching for objects where a single value must be matched with many patterns. **Example** To search for all objects with names starting with the characters “abc” and ending with “xyz”, specify the Property Key name and the Value abc*&&*xyz.
\ (Back Slash)	This is used when the name of the object itself contains a comma. This character is called an escape sequence, since it avoids searching of the objects, as if it were two different names. **Example** To search for an object with name “a,b”, specify the Property Key name and the Value a\,b.
<between>"value1" and "value2"	Used for objects with numeric values within a specific range. **Example** To search for objects with a poll interval value ranging from 300 to 305, specify the property key as poll interval and the Value as 300 and 305 Note that the first number must be smaller than the second number. Only the values between and including the given values, are matched.

Deleting an authorized custom view scope

To delete the authorized scopes associated with a Custom View Scope completely from the database, follow these steps:

To delete the authorized scope associated with a custom view scope, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

2 Select the required group under the Groups node in the Security tree.

3 Click the **Custom View Scope for Group** tab in the right-hand panel.

4 Select the required Custom View Scope Name from the drop-down menu.

5 Select the required Authorized Scope row to be deleted and right-click the row to launch the popup menu.

6 Select the **Delete AuthorizedView** menu item to remove the selected Authorized Scope.

Note: Selecting **Delete AuthorizedView** deletes the Authorized Scope completely which is associated to the groups. Hence, to delete an Authorized Scope set for a custom view scope from the selected group alone, click the **Assign Authorized Scope** button and dissociate it from the currently selected group.

Using the Operations tree

The Security Administration tool contains a list of all the authorized Integrated EMS operations logically arranged in a tree structure, with parent and child operations. If the Integrated EMS applications change (new applications are added or old applications are no longer used), the Integrated EMS administrator must modify the Operations tree so that any new operations are authorized for assigning to users or groups. Integrated EMS administrator can make these changes using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the "Starting the Security Administration tool").
2. Select the **File-->New-->AddOperations** menu command.

   This opens the Operations dialog.

The tasks relating to the Operations Tree are as follows:

- Adding new operations
- Deleting an operation

Adding new operations

In future, it is possible to add a new application to the Integrated EMS. Then new operations can be included for the (newly) added applications in the Integrated EMS. For these operations to be authorized, they have to be present in the Operations dialog of the Security Administration tool.This section explains the steps to add operations to the OperationsTree.

To add a new operation to the Operations Tree, follow these steps:

In the Security Administration tool of Integrated EMS

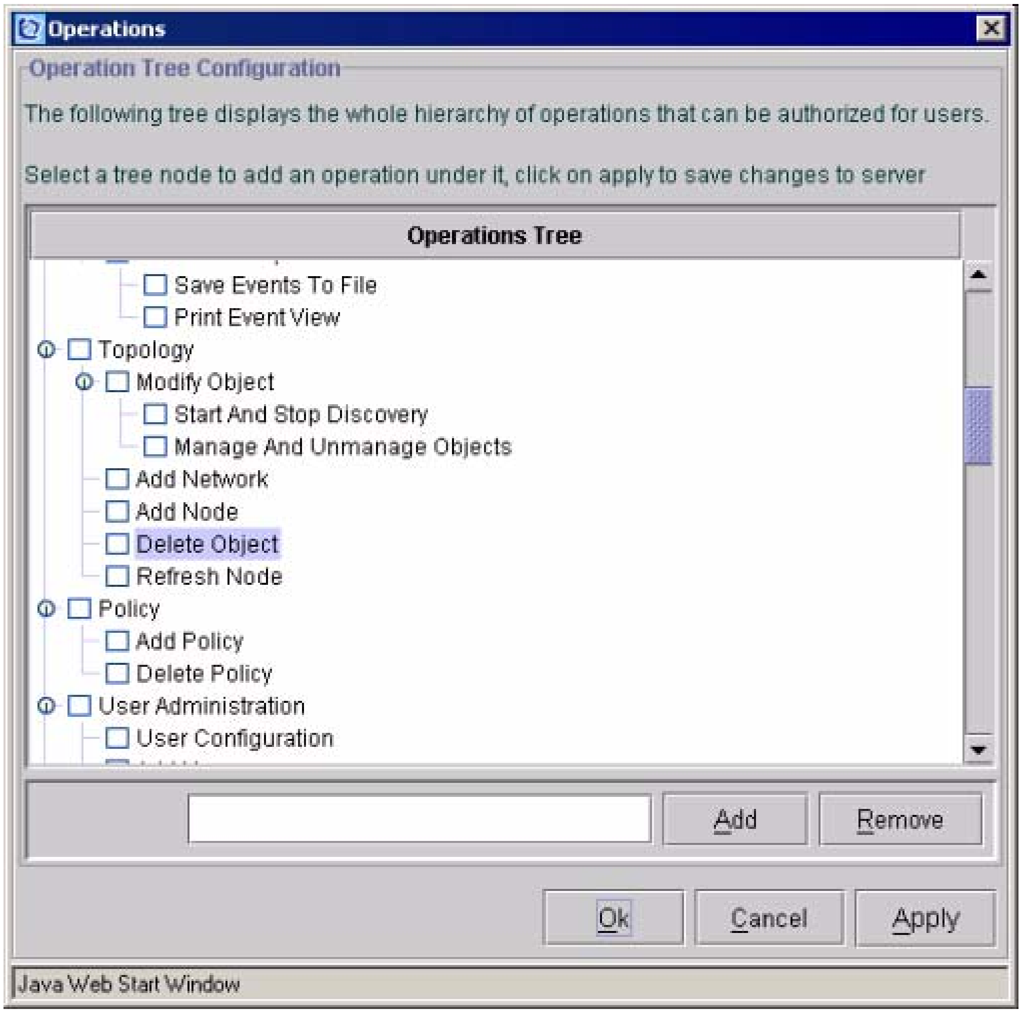
1 Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 Select the **File-->New-->AddOperations** menu command.

OR

Click the **Operations** button in the toolbar.

This Operations dialog opens, as shown in the following figure.



The following tree displays the whole hierarchy of operations that can be authorized for users.

Select a tree node to add an operation under it, click on apply to save changes to server

- □ Save Events To File
- □ Print Event View
- □ Topology
  - □ Modify Object
    - □ Start And Stop Discovery
    - □ Manage And Unmanage Objects
  - □ Add Network
  - □ Add Node
  - □ Delete Object
  - □ Refresh Node
- □ Policy
  - □ Add Policy
  - □ Delete Policy
- □ User Administration
  - □ User Configuration

3 Select the tree node under which the new operation is to be added.

4 Type the name of the operation and click the **Add** button.

The system displays the new operation under the selected parent operation in the Operation Tree.

5 Click the **Apply** button to add the operation.

6 Click the **OK** button to update the operation details in the Integrated EMS Server.

7 Repeat steps 4, 5, and 6 to add further operations.

Deleting an operation

If the Integrated EMS applications change, the Integrated EMS administrator must delete any unused operations from the Operations Tree.

To delete an operation from the Operations Tree, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the "Starting the Security Administration tool").
2. Select the **File-->New-->AddOperations** menu command to launch the Operations dialog.
3. Select the operation to be deleted from the Operations Tree and click the **Remove** button.

   The system removes the operation from the Operations Tree after confirmation for removal.
4. Click the **OK** button to confirm the deletion and update the operation details in the Integrated EMS Server. Alternatively click the **Apply** button to continue with other tasks in the Operations dialog.

Configuring security management parameters

Integrated EMS administrator can configure various security management parameters, including a parameter to control the maximum number of login attempts. Integrated EMS holds a value for the maximum allowed number of login attempts. When a user's unsuccessful login attempts exceed this value, the user is not allowed to log into the network. Integrated EMS stores the maximum value in the parameter maximum_allowed_login_failed_count of NMSProcessesBE.conf file in <IEMS Home>/conf, where <IEMS Home> is the home directory of the Intgrated EMS installation directory.

Maximum allowed failed login attempts

Integrated EMS administrator can configure the maximum allowed login attempts by changing the parameter maximum_allowed_login_failed_count available in the process com.adventnet.nms.security.authentication.NmsAuthenticationManager.

To configure the maximum allowed login attempts in Integrated EMS, follow these steps:

At Integrated EMS Server workstation

1 Navigate to <IEMS Home>/conf in the system where the Integrated EMS Server is installed.

2 Open the NMSProcessesBE.conf file using a standard text editor (for example, “vi” in Sun Solaris).

3 Type the required value at the end of the login_failed_count command string.

Example
To set the maximum as 4, the command is:

```
#java
com.adventnet.nms.security.authentication.NmsAuthenticationManager [AuthenticationImpl]
[maximum_allowed_login_failed_count] PROCESS
com.adventnet.nms.security.authentication.NmsAuthenticationManager ARGS NULL 4
```

Note: The default value is zero. This means that unless the Integrated EMS administrator configures the parameter, there is no limit on the number of unsuccessful login attempts by the user.

Configuring client lock out

Integrated EMS administrator can configure the client lock-out time by specifying the time period (in minutes) for the ALLOWED_IDLE_TIME_BEFORE_LOCKOUT attribute in clientparameters.conf file located in <IEMS Home>/conf directory. If the Integrated EMS client remains in the idle state for the configured time period, then it gets locked out.The default time period for the Integrated EMS client to remain idle before locking out is 10 minutes. The client can again be accessed by authenticating it with user ID and password.

To configure the client lock-out time period in Integrated EMS, follow these steps:

At Integrated EMS Server workstation

1 Navigate to <IEMS Home>/conf in the system where the Integrated EMS Server is installed.

2 Open the clientparameters.conf file using a standard text editor (for example, “vi” in Sun Solaris).

3 Type the required value at the end of the ALLOWED_IDLE_TIME_BEFORE_LOCKOUT command string.

Example
To set the maximum as 15 minutes, the command is:
ALLOWED_IDLE_TIME_BEFORE_LOCKOUT="15"

As per this configuration, the Integrated EMS client is locked out when it remains in the idle state for more than 15 minutes.

Understanding Integrated EMS Administrative operations

The Operations Tree contains a list of operations that are provided by default on Integrated EMS server. One of the Integrated EMS administrator's functions is to assign different operations to different users.

The operations in Integrated EMS are listed below:

- Administrative operation
- Events
- Topology
- Job
- User administration
- Alerts
- Maps
- Threshold objects

> ***Note:*** The following operations displayed in *Operations* dialog are not used in Integrated EMS.
>
> - Trap Parsers and Filters
> - Configuration
> - Polling Units
> - Polling Objects
> - Poll Filter
> - Provisioning

Administrative operation

This section describes the various administrative operation that can be added or removed using the Operations dialog in Security Administration tool.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.
2. Select the **File-->New-->AddOperations** menu command.

   This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the Administration node in the *Operations* dialog:

Description of operations under the Administration Operation node of the Operations dialog

Operation	Description
Clear Discovery	This operation is used when the Discovery process is stopped abruptly for any reason.
Start Backup	This operation starts the backup process by setting the BackUpInProcess variable to true and suspends all Integrated EMS Server schedulers. When the backup process is over, it automatically resets the BackUpInProcess variable to false, to resume Integrated EMS Server schedulers.
Resume Integrated EMS Server	This operation can be used to resume all the Integrated EMS Server schedulers, if Integrated EMS Server hangs because of some unforeseen problems during the backup process.
Shutdown Integrated EMS Server	This operation is used for shutting down the Integrated EMS Server with authentication.
Configure Log Levels	This operation can be used to set the logging and the corresponding levels for various modules in the Integrated EMS Server.
Runtime Administration	This operation is a powerful tool to configure the Integrated EMS Server settings from the Integrated EMS without a need for the user to restart the server for the new settings to take effect.

Description of operations under the Administration Operation node of the Operations dialog

Operation	Description
Security Administration	Security Management is about authenticating a user from logging into Integrated EMS to provide permissions to perform operations.
System Administration	This Operation is the entry point for all administrative operations.

Note: If any of the above operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Events

Network events are entities that represent the various changes of status of the objects managed by Integrated EMS. Events can convey either general information or the current status of the managed objects. This section describes the operations related to events that can be added or removed using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.

2 Select the **File-->New-->AddOperations** menu command.

This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the Events node in the *Operations* dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Events node of Operations dialog

Operation	Description
Event Filters And Parsers	
Get Event Parsers	This operation is for viewing the Event Parsers present in the server.
Set Event Parsers	This operation is for modifying existing Event Parsers or creating a new Event Parser.
Get Event Filters	This operation is for viewing the Event Filters present in the server.
Set Event Filters	This operation is for modifying existing Event Filters or creating a new Event Filter.
Event User Operations	

Description of operations under the Events node of Operations dialog

Operation	Description
Save Events To File	This operation is for saving the selected events or the events displayed in the Events Panel.
Print Event View	This operation is for printing either the selected events or events displayed in the Events Panel.

Topology

This section describes the various topology operations that can be added or removed using the Operations dialog in the Security Administration tool. The topology-related operations include adding, updating, deleting, and filtering out the core managed objects from the Integrated EMS Server database.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.

2 Select the **File-->New-->AddOperations** menu command.

This opens the *Operations* dialog.

The following table provides descriptions of the operations under the Topology node in the Operations dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Topology Node of the Operations dialog

Operation	Description
Modify Object	
Start and Stop Discovery	This operation is used to set the discovery status for the particular object at run time.
Manage and Unmanage Objects	This operation is used to set the management status of the particular object at run time.
Add Network	This operation is used to add a new network in the topology.
Add Node	This operation is for adding a new node in the topology.
Delete Object	This operation is for removing a particular object from the topology.

Description of operations under the Topology Node of the Operations dialog

Operation	Description
Modify Object	
Refresh Node	This operation is for updating the status polling.
ASCII Dump	This operation is used to collect the list of discovered devices from the topology database and print them in a text file.

Job

Jobs are tasks that are executed by the Integrated EMS Server at a system level, at a specified period of time. Whenever there is a requirement to send notifications to the Integrated EMS Server at run time, jobs are executed. This section describes the operations related to jobs that can be added or removed using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the “Starting the Security Administration tool” for more details.

2 Select the **File-->New-->Add Operations** menu command.

This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the Job node in the *Operations* dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Jobs node of the Operations dialog

Operation	Description
Add Job	This operation is for creating a new job.
Delete Job	This operation is for removing an existing job from the system.

User administration

This section describes the various User Administration operations that can be added or removed using the Operations dialog in the Security Administration tool.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.
2. Select the **File-->New-->AddOperations** menu command.

   This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the under the User Administration node in the *Operations* dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the User Administration node of Operations dialog

Operation	Description
User Configuration	This operation is used to obtain the link for User Administration.
Add Users	This operation is used to create a new user.
Assign User To Group	This operation is used to assign the user to a new or existing group.
Remove Users	This operation is used to remove the whole account for a particular user.
Remove User From Group	This operation is used to remove the particular user from a particular group only.
Change Password	This operation is used to change the existing password for a particular user.
Get List of Users	This operation is used to view the list of users present in the database.
Set User Permission	This operation is used to sets operations or permissions for the existing users.

Description of operations under the User Administration node of Operations dialog

Operation	Description
Set User Profile	This operation is used to set profiles for the existing users.
Clear Audit Trails	This operation is used for clearing audit trails for the user.

Alerts

Alerts or alarms are generated when a failure or fault is detected in the managed objects. The system displays the generated alarms in the Integrated EMS alarms panel. This section describes the operations related to alarms that can be added or removed using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.

2 Select the **File-->New-->AddOperations** menu command.

This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the Alarms node in the Operations dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Alerts node of the Operations dialog

Operation	Description
Alert Filters	
Get Alert Filters	This operation is for viewing the alert filters present in the server.
Set Alert Filters	This operation is for modifying existing alert filters or for creating a new alert filter
Alert User Operations	
Set Alert Annotation	This operation is for adding notes to an alarm.
Get Alert Details	This operation is for viewing the details of a particular alarm.
Save Alerts To File	This operation is for saving either the selected alarms or the alarms displayed in the current alarm panel into a file.
Print Alert View	This operation is for printing either the selected alarms or the alarms displayed in the current alarm panel.

Description of operations under the Alerts node of the Operations dialog

Operation	Description
Clear Alerts	This operation is for changing the alarm severity to Clear.
Get Alert Annotation	This operation is for viewing a particular existing alarm annotation.
Get Alert History	This operation is for viewing the alarm history, that is, the change in status of an alarm from the first alarm to the latest alarm.
Alert Pickup	This operation is used to pick up the alarm.
Delete Alarms	This operation is used to remove a particular alarm, which is of no interest or has been resolved.

Maps

Map or topology is a graphical representation of objects in the Integrated EMS clients. This section describes the operations related to maps that can be added or removed using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.

2 Select the **File-->New-->AddOperations** menu command.

This opens the *Operations* dialog.

The following table provides descriptions of the various operations under the Maps node in the *Operations* dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Maps node of the Operations dialog

Operation	Description
Map Editing Operations	This operation is mainly used to configure maps, such as the creation of new maps, customizing map hierarchy, map symbol layout, and map symbol renderers in the Integrated EMS.

Threshold objects

Threshold objects are statistical values associated with the collected data.This section describes the operations related to events that can be added or removed using the Operations dialog.

To launch the Operations dialog, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool. Refer to the "Starting the Security Administration tool" for more details.

2 Select the **File-->New-->AddOperations** menu command.

This opens the Operations dialog.

The following table provides descriptions of the various operations under the Threshold Object node in the *Operations* dialog:

> ***Note:*** If any of the below operation is to be restricted for a user, it can be disabled by checking **X** in the check box.

Description of operations under the Threshold Object node of the Operations dialog

Operation	Description
Add Threshold Object	This operation is used for adding new threshold objects.
Modify Threshold Object	This operation is used for modifying the existing threshold objects.
Delete Threshold Object	This operation is used for removing the threshold objects.
Get Threshold Objects	This operation is used for viewing the existing threshold objects.

Centralized security administration overview

Integrated EMS provides centralized authentication, administration, and authorization for most components in the solution.

Integrated EMS provides security architecture based on a Pluggable Authentication Module (PAM) and Name Services Switch (NSS).

This architecture provides the following features:

- central administration of user accounts
- central authentication. Authentication of centrally administered user accounts is performed by the central security server.
- central authorization. Authorization information needed to support user access control is securely managed and provided by the central security server.
- single sign-on (SSO). This capability enables the user to access multiple network elements, applications, and features from a single login session. Session information for a user is shared between Integrated EMS and networks elements which support SSO.
- the ability to plug in a third-party authentication or authorization solution
- the ability to generate centralized security logging for successful and failed authentications

The following table lists the devices and applications that support central security administration features.

> ***Note:*** To configure a device to use centralized security, refer to the documents listed in the following table. You should configure a device to use central security, only after the Integrated EMS central security server has been configured and activated in the network.

Central security administration - supported devices

Network element/EMS platform	Device authentication method	Documentation reference
USP	HTTPS	USP Security and Administration, NN10159-611
Passport 8600	Radius	Configuring and Managing Security, 314724-B

Central security administration - supported devices

Network element/EMS platform	Device authentication method	Documentation reference
SSPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	PAM	ATM/IP Solution-level Security and Administration, NN10402-600
Integrated EMS	HTTPS	Integrated EMS Security and Administration, NN10336-611
CICM Manager	HTTPS	CICM Configuration Management, NN10240-511

The following table lists Integrated EMS single sign-on launch points.

Integrated EMS single sign-on launch points

Network element/EMS platform/application	Integrated EMS launch point
USP	USP Command Line USP Manager
Passport 8600	PP8600 Command Line
SSPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	CS 2000 Management Tools
SAM21 Manager	SAM21 Manager
UAS Manager	UAS Manager
LMM	LMM
TMM	TMM
OSSGate	OSSGate BPT Servlet BPT Command Line

Integrated EMS single sign-on launch points

Network element/EMS platform/application	Integrated EMS launch point
MG9000 Manager MG9000 Mid-Tier	MG9000 Manager
APS	APS Manager APS Application
NPM	NPM NPM Command Line
QOS	QOS Command Line
SSPFS	SSPFS Command Line

Authentication and authorization

Network elements and applications can be configured to use centralized security administration. To enable a device to use centralized security administration, the device must be configured to use the Integrated EMS central security server to authenticate users and access user profile information.

Integrated EMS Central Security Server uses PAM to process the authentication requests and NSSwitch to return user privilege and user profile information to network elements and applications.

PAM services

PAM provides authentication services for clients in the managed network. Customers have the option to use the PAM services that come pre-bundled with the security server or to provide their own. For details on configuring PAM, see Configuring the Integrated EMS central security server in the network.

When a request is forwarded to the Integrated EMS PAM Service Provider (SPI), then authentication is performed against data provisioned and administered by the security administration application on the Integrated EMS client.

Conversely, when PAM services are provided by a customer, incoming authentication requests are forwarded to the customer SPI for resolution against their remote database.

NSSwitch services

NSSwitch provides services to obtain group and profile information for users. Centralized access to network resources depends on the definition of a common set of user groups to map security access for each user. The Nortel Networks solution provides a number of predefined user groups to address the full range of OAM&P functions required across a managed network. For details of these user groups and their categorization, see the User groups section of Setting up local user accounts on a Sun server.

Customers can configure NSSwitch to use the service pre-bundled with Integrated EMS or, as with PAM services, provide their own service remotely. When the pre-bundled service is used, group and user profile information is administered from command-line Unix interface on the Integrated EMS server. For details, see Configuring a third-party Pluggable Authentication Module.

If NSSwitch services are configured on a third party system, it is important to note that this security solution supports only the NSSwitch group and password databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

Single sign-on (SSO)

The single sign-on feature allows users transparent access to multiple network elements and applications through a single login. Once a user has been successfully authenticated for the first time (by user login), an SSO token is created by the Integrated EMS security server that will be used to authenticate the same user on subsequent login attempts.

Network elements and applications use a single sign-on (SSO) interface on the central security server to request SSO tokens whenever authentication is required.

Hardware requirements

The following table lists details of port usage.

	Port details
Security server	
Radius server	1812 (UDP/Radius authentication)
Apache/Tomcat Apache/Tomcat (SSL)	80:8080 443/8443

	Port details
SunONE IS	58080, 58081 (TCP for Radius and HTTPS proxies) 58888, 7000 (TCP/logging)
SunONE web services	389 (UDP/LDAP/DS) 2413 (TCP/LDAP)
SSPFS client	
Pam-radius daemon	dynamically allocated port from available ports for programs (range 5,000 - 65,535)

Limitations and restrictions

The following are limitations and restrictions:

- the following devices do not support centralized security administration in (I)SN07: Succession Core and Billing Manager (CBM), Preside MDM, Media Gateway 7400/15000, Multiservice Switch 15000
- the maximum number of provisional central security users is 1000
- if you set the status of a newly created user to “disable” in the User Profile dialog box, the Integrated EMS Security administration tool can take up to 24 hours to disable command line access to the Integrated EMS server. You can disable an account immediately by setting the user’s shell to /bin/false. To set the user’s shell to /bin/false, log in to the Integrated EMS server as root and type the command usermod -s /bin/false <username>.
- due to update time intervals, it may take up to 30 minutes after an account or password expires for the expiry to be displayed in the Integrated EMS Security Administration window
- third party pluggability is supported for DCE client version 3.2, patch PTF6 for DCE and SunONE directory server 5.1 for LDAP
- for third party pluggability, the only pam.conf edits that are supported are pam_dce and pam_ldap
- password aging notification is not supported on any centralized security devices or on the security server in (I)SN07
- on a client SSPFS machine, updates to user profile and group information that are performed on the security server are applied when a user exits all SSPFS client sessions on the client machine and logs back into the client machine

- on SSPFS devices, you must set up SSPFS platform access to enable user platform access to the device
- Succession Centrex IP Client Manager Element Manager (CICM) only supports central authentication. CICM Manager does not support single sign-on (SSO).
- The procedure for deleting a user’s central account must be followed. If the procedure for Disabling or deleting a user session is not followed correctly
  - the user’s home directories may be accessible to a new user who inherits the same user ID as the original user
  - the new user who inherits the same user ID as the original user will not be able to log in to the SSPFS security clients
- telnet access to the Integrated EMS server is restricted to local accounts only
- a certificate must be installed on the Integrated EMS server to ensure that the system operates correctly
- Integrated EMS allows you to configure user ID ranges. Sun Solaris security clients such as SSPFS use a user ID to uniquely identify a user. The default Integrated EMS user ID range is 10001-12000. You can change the Integrated EMS user ID. You must ensure that there is no conflict between the new Integrated EMS user ID range and the Sun Solaris system user ID range in /etc/password. Such a conflict may severely impact system operation. The following table lists Sun Solaris system accounts and user IDs.
- the total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created at the SSPFS/Solaris level.
- the user name cannot be longer than 8 characters.
- the group name cannot be longer than 8 characters.

Sun Solaris system accounts and user IDs
root:0, daemon:1, bin:2, sys:3, adm:4, lp:71, uucp:5, nuucp:9, listen:37, nobody:60001, noaccess:60002, nobody4:65534, sshd:100, maint:101, npm:102, npmftp:103, ptm:104, mgems:105, www:106, patcher:107, poller:108, certuser:109, sam21em:110, anonymous:111, image:112, pfrs:113, mtssg:50015, FIELD:50016, oracle:50017, patch:50018

Configuring the Integrated EMS central security server in the network

Application

Use this procedure to configure and activate the Integrated Element Management System (EMS) central security server in the network. The Integrated EMS acts as a proxy to the central security administration system.

ATTENTION

Only one Integrated EMS central security server can be configured in the network.

ATTENTION

Reverting to the previous configuration of the server is not supported. A rollback of the Succession Server Platform Foundation Software (SSPFS) must be performed to revert the security server to its previous configuration.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated Element Management System (EMS) is already installed or upgraded on the server, and it is running Succession Server Platform Foundation Software (SSPFS) release (i)SN07 or greater
- an HTTPS certificate is already installed on the server (refer to procedure Installing an HTTPS certificate on an SSPFS-based server on page 121, if required)
- the SunONE component is already configured to run in secure mode (refer to procedure Configuring the security server SunONE component on page 116, if required)

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server where Integrated EMS resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Migrate the user accounts you want to centrally manage, from the local security database on the SSPFS-based server to the central administration system as follows:

Note 1: It is recommended to migrate all user accounts that exist on SSPFS-based servers to the central administration system with the following exceptions:

root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.

Note 2: If the central security administration application is a third-party application and not the Integrated EMS, follow the procedures in the third party documentation.

a Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

b Note the user groups the user currently belongs to.

c Delete the user accounts you want to centrally manage, from the Unix files on the server.

> ***Note:*** In a two-server configuration, delete the user accounts on both servers (inactive and active).

Delete a user account by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

Repeat this step for each user account you want to centrally manage.

d If the central administration system is the Integrated EMS, launch the Security Administration tool of the Integrated EMS, and add the user accounts you want to centrally manage. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611.

> ***Note:*** All users added through the Integrated EMS Security Administration tool, are by default assigned to the “succssn” user group for login access.

e If the central administration system is the Integrated EMS, assign the user account group information in Unix.

> ***Note:*** In a two-server configuration, assign the user account group information on both servers (inactive and active).

Assign one or more user groups to a user by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups below)

Include a comma between groups, but no space.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

userid
is a variable for the user name

> ***Note 1:*** Do not set the Unix password for the user account.

> ***Note 2:*** The total number of groups that a user can belong to, cannot exceed sixteen. The sixteen groups include groups created in Integrated EMS and groups created in SSPFS/Solaris.

6 Complete PAM configuration as follows:

At installation, the Integrated EMS replaces the existing PAM configuration file (pam.conf) with a new PAM configuration file that uses the Integrated EMS security application. If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

You can use the Integrated EMS PAM, which is pre-bundled with the Integrated EMS load, or you can use your own third-party PAM. The Distributed Computing Environment (DCE) and the Lightweight Directory Access Protocol (LDAP) PAMs are the third-party PAMs that are supported. Refer to procedure Configuring a third-party Pluggable Authentication Module on page 101, if required.

7 Once PAM configuration is complete, add PAM Radius (Remote Access Dialup User Service) clients to the Radius server as follows:

> ***Note:*** Clients cannot authenticate through the security server if the client IP is not added through the Radius Client Configuration command line interface (CLI).

In a two-server configuration, perform the steps that follow on both servers (inactive and active).

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS security server

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

e Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

select -
```

f Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

g Enter the number next to the “Succession Element Configuration” option in the menu.

Example response

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SESM Application Configuration
 3 - SAM21EM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration
 7 - RADSVR Application Configuration
 8 - S1IS Application Configuration

 x - exit

select -
```

h Enter the number next to the “RADSVR Application Configuration” option in the menu.

Example response

```
RADSVR Application Configuration
 1 - LIST_CLIENTS (List all of the existing
     Radius clients)
 2 - DELETE_CLIENTS (Delete a Radius client)
 3 - ADD_CLIENTS (Add clients to the Radius
     server)

 x - exit

select -
```

i Enter the number next to the “ADD_CLIENTS” option in the menu.

Example response

```
===Executing “ADD_CLIENTS”

Enter radius client IP or subnet to ADD (“end
to terminate):
```

j When prompted, enter the radius client IP or subnet you want to add.

Example response

```
Enter radius client shared secret:
```

k When prompted, enter the radius client shared secret.

Example response

```
Enter radius client type:
```

l When prompted, enter the radius client type (for example, IEMS).

Example response

```
Adding Radius server client: 12.45.33.74
Enter radius client IP or subnet to ADD (“end”
to terminate)
```

m When prompted, enter the IP address or subnet of the radius client you want to add.

> ***Note:*** For a two-server configuration, you must enter the two physical IP addresses of the cluster as well as the virtual IP address of the SSPFS-based host. For a one-server configuration, enter the virtual IP address of the SSPFS-based host.

n Complete the add process by typing

end

and pressing the Enter key.

Example response

```
Reload Radius server dynamic configuration
files...
Radius server dynamic configuration reload
successful.

===”ADD_CLIENTS” completed successfully
```

o Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

Configuring a central security client

Application

Use this procedure to configure a central security client to use the Integrated Element Management System (Integrated EMS) central security server. A central security client is an Succession Server Platform Foundation Software (SSPFS)-based server that hosts the Operations, Administration, Maintenance, Performance (OAM&P) applications, such as the Media Gateway (MG) 9000 Manager, CS 2000 Management Tools, and CS 2000 SAM21 Manager.

ATTENTION

You can revert to the previous configuration of the client server using procedure Reverting the client server to its previous configuration on page 112.

In the event you want to re-configure the central security client to use a new Integrated EMS server IP, perform steps 2 and 3 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated EMS central security server is already configured and activated in the network (refer to procedure Configuring the Integrated EMS central security server in the network on page 82, if required)

Action

Perform the following steps to complete this procedure.

At your workstation

1 Migrate the user accounts you want to centrally manage, from the local security database on the SSPFS-based client to the central administration system as follows:

> ***Note 1:*** It is recommended to migrate all user accounts that exist on SSPFS-based servers to the central administration system with the following exceptions:
>
> root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.
>
> ***Note 2:*** If the central security administration application is a third-party application and not the Integrated EMS, follow the procedures in the third party documentation.

a If the central administration system is the Integrated EMS, launch the Security Administration tool of the Integrated EMS, and add the user accounts you want to centrally manage. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611.

> ***Note:*** All users added through the Integrated EMS Security Administration tool, are by default assigned to the *succssn* user group for login access.

b If the central administration system is the Integrated EMS, assign the user account group information in Unix.

Log in to the Integrated EMS central security server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS central security server

c When prompted, enter your user ID and password.

d Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

e When prompted, enter the root password.

f Assign the user account group information in Unix.

> ***Note:*** In a two-server configuration, assign the user account group information on both servers (inactive and active).

Assign one or more user groups to a user by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups below)

include a comma between groups, but no space

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

userid
is a variable for the user name

Note: Do not set the Unix password for the user account.

g Delete the user accounts you just added to the Integrated EMS central security server.

> ***Note:*** In a two-server configuration, delete the user accounts on both servers (inactive and active).

Log in to the client server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based client server

h When prompted, enter the user ID and password for an account that was migrated to the Integrated EMS central security server.

i Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

j When prompted, enter the root password.

k Delete the user account by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

Repeat this step for each user account you migrated to the Integrated EMS central security server.

2 Configure the Integrated EMS security server location as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

select -
```

b Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

d Enter the number next to the “IEMS Server Location Configuration” option in the menu.

Example response

```
IEMS Server Location Configuration
 1 - iems_ip (Configure IEMS Server IP)

 x - exit

select -
```

e Enter the number next to the “iems_ip” option in the menu.

Example response

```
===Executing “iems_ip”

Enter the IEMS Server IP Address (default
0.0.0.0):
```

f When prompted, enter the virtual IP address of the Integrated EMS server.

Example response

```
IEMS IP: 45.12.23.56

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

g Accept the IP address you just entered by typing

ok

and pressing the Enter key.

Example response

```
=== “iems_ip” completed successfully
```

h Return to the Security Services Configuration menu, by typing

```
select - x
```

and pressing the Enter key.

Response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

3 Configure PAM as follows:

a Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

 x - exit

select -
```

b Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 x - exit

select -
```

c Enter the number next to the “pam_radius” option in the menu.

Example response

```
===Executing “pam_radius”

Saving original PAM configuration

Updating PAM Configuration to use IEMS
Security Server
IEMS Security Server IP: 45.12.23.56

Enter “ok” to continue
Enter anything else to exit
```

d Accept the PAM configuration update by typing

ok

and pressing the Enter key.

Example response

```
Enter the Shared Secret
```

e When prompted, enter the security server shared secret.

f Accept the shared secret you just entered by typing

ok

and pressing the Enter key.

g When prompted, enter the Radius Client timeout, or press the Enter key to accept the default value if one is specified.

Example response

```
Radius Client Timeout: 12

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

h When prompted, accept the update by typing

```
ok
```

and pressing the Enter key.

Example response

```
Configuring pam-radius
Starting pam-radius
===”pam_radius” completed successfully
```

The system replaces the existing PAM configuration file (pam.conf) with a new PAM configuration file that uses the Integrated EMS security server.

i Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

j If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

4 Set up SSPFS platform access for users that are centrally managed as follows:

> ***Note:*** Users that are centrally managed, must have their environment set up on the SSPFS platform they have access to, to access that SSPFS platform through telnet, SSH, or other supported login utilities. Only perform this step if users are to be granted platform access.

In a two-server configuration, perform the steps that follow on both servers (active and inactive).

a Log in to the Integrated EMS central security server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS central security server

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d When prompted, enter the root password.

e Set up the user’s shell and home directory by typing

```
# usermod -s /bin/sh -d
/export/home/<username> <username>
```

and pressing the Enter key.

where

username
is the user’s ID

Note: The above command is entered on one line.

f Determine the user’s user ID (UID) by typing

```
# id <username>
```

and pressing the Enter key.

where

username
is the user’s ID

Note: A user’s UID is autogenerated when the user’s account is created.

g Log in to the SSPFS-based server the user has access to by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server the user has access to

h When prompted, enter the user’s ID and password.

i Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

j When prompted, enter the root password.

k Set up the user's UID on the SSPFS-based server by typing

```
# useradd -u <uid> <username>
```

and pressing the Enter key.

where

uid
is the user's UID you obtained in step 4f.

username
is the user's ID

l Set up the user's home directory on the SSPFS-based server by typing

```
# mkdir /export/home/<username>
```

and pressing the Enter key.

where

username
is the user's ID

m Change the ownership of the user's home directory by typing

```
# chown <username> /export/home/<username>
```

and pressing the Enter key.

where

username
is the user's ID

n Log out of the SSPFS-based server by typing

```
# exit
```

and pressing the Enter key.

5 You have completed this procedure.

Configuring a third-party Pluggable Authentication Module

Application

Use this procedure to configure a third-party Pluggable Authentication Module (PAM) on the Integrated Element Management System (EMS) central security server. Both of the following third-party Pluggable Authentication Modules (PAMs) are supported:

- Distributed Computing Environment (DCE) PAM
- LIghtweight Directory Access Protocol (LDAP) PAM

Prerequisites

To perform this procedure, you need to have the root user ID and password for the Integrated EMS central security server, and either the DCE or LDAP prerequisites below depending on which third-party PAM you are configuring.

DCE prerequisites

The following prerequisites apply to DCE PAM:

- To configure the DCE PAM, you need administrative privileges for the DCE server.
- DCE must already be configured on the server. If required, refer to procedure “Configuring DCE on a Sun server” in the ATM/IP solution-level Configuration Management document, NN10409-500.

Note: For DCE to function correctly, DCE client 3.2 must be installed and patch PTF6 must be applied. Patches are available at the following link: https://www6.software.ibm.com/dl/dcesol/dcesol-p.

LDAP prerequisites

To configure LDAP PAM, an LDAP server must already be configured with support for Solaris Native LDAP schema.

Note: Information on LDAP schema, is available at the following link: http://docs.sun.com/db?q=ldap+configuration+guide&p=doc%2F806-5580

Action

Perform the following steps to complete this procedure.

Distributed Computing Environment (DCE) PAM

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS central security server on which you want to change the PAM

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Disable the Name Service Cache daemon as follows:

a Stop the Name Service Cache daemon

```
# /etc/init.d/nscd stop
```

and pressing the Enter key.

b Move the “/etc/nscd.conf” file to a different location.

6 Add “dce” as another option for the password and group in the “/etc/nsswitch.conf” file.

The entries would look similar to “passwd: files nis dce” and “‘group: files nis dce” after the change.

This enables the group information to come from DCE.

7 Enable the DCE naming service server by typing

```
# config.dce nsswitch
```

and pressing the Enter key.

8 Enable the DCE PAM (Pluggable Authentication Module) by typing

```
# config.dce pam
```

and pressing the Enter key.

9 Edit the /etc/pam.conf file as follows:

a Add pam_dce with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "login auth" to "login auth sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "other auth" to "other auth sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "sesm auth" to "sesm auth sufficient /usr/lib/security/$ISA//pam_dce.so.1 try_first_pass"
- change "secclient auth" to "secclient auth sufficient /usr/lib/security/$ISA//pam_dce.so.1"

b Add pam_dce with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "login account" to "login account sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "other account" to "other account sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "sesm account" to "sesm account sufficient /usr/lib/security/$ISA//pam_dce.so.1 try_first_pass"
- change "secclient account" to "secclient account sufficient /usr/lib/security/$ISA//pam_dce.so.1"

c Add pam_dce with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "sesm session" to "sesm session sufficient /usr/lib/security/$ISA//pam_dce.so.1 try_first_pass"
- change "secclient session" to "secclient session sufficient /usr/lib/security/$ISA//pam_dce.so.1"

d Add pam_dce with sufficient setting as the first entry in the pam.conf" file as indicated:

- change "other password" to "other password sufficient /usr/lib/security/$ISA//pam_dce.so.1"
- change "sesm password" to "sesm password sufficient /usr/lib/security/$ISA//pam_dce.so.1 try_first_pass"
- change "secclient password" to "secclient password sufficient /usr/lib/security/$ISA//pam_dce.so.1"

e Remove the "other password" entry for iems in the "etc/pam.conf" file.

10 Add the users and permissions to the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611

11 Disable the users’ status in the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Setting a user profile” in the Integrated EMS Security and Administration document, NN10336-611, for instructions on how to disable a user’s status.

12 Add users and user groups to DCE as follows:

Note: For details on user groups, refer to procedure Setting up local user accounts on a Sun server.

a Log in to DCE using the cell_admin user ID and password.

b Add a user to DCE by typing

```
dcecp> user create <userid> -group succssn
-password <password> -organization
ossaps-users -mypwd <cell_admin_password>
```

and pressing the Enter key.

where

userid
is the user ID of the user you want to add

password
is the password for the user ID you want to add

cell_admin_password
is the password for cell_admin

Note: The above command is entered on one line.

c Add the necessary user groups in DCE by typing

```
dcecp> group create <groupname>
```

and pressing the Enter key.

where

groupname
is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- trkro, lnro, mgcro, mgro, emsro

d Add the new users to the new groups, one at a time, by typing

```
dcecp> group add <groupname> -member <userid>
```

and pressing the Enter key.

where

groupname
is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- trkro, lnro, mgcro, mgro, emsro

userid
is the user ID of a new user

e Verify the user was added by typing

dcecp> **group list <groupname>**

and pressing the Enter key.

where

groupname
is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnsprov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmtc, mgmtc, emsmtc
- trkro, lnro, mgcro, mgro, emsro

f Activate the new user by typing

dcecp> **acct modify -acctvalid yes <userid>**

and pressing the Enter key.

where

userid
is the user ID of a new user

13 You have completed this procedure.

Note: When the DCE authentication mechanism is selected, you must use the UNIX passwd command with the “-r” option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “`passwd -r file <userid>`”.

LIghtweight Directory Access Protocol (LDAP) PAM

At the LDAP server

1 Add the users and permissions to the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611

2 Disable the users’ status in the Integrated EMS using the Integrated EMS Security Administration tool. If required, refer to procedure “Setting a user profile” in the Integrated EMS Security and Administration document, NN10336-611, for instructions on how to disable a user’s status.

3 Add users and user groups to LDAP server as follows:

Note: For details on user groups, refer to procedure Setting up local user accounts on a Sun server.

a Log in to the LDAP server.

b Add the necessary user groups to the LDAP server. The user groups are listed below with their corresponding group ID.

- succssn:105
- trkadm:1001, trkrw:1002, trksprov:1003, trkmtc:1004, trkro: 1005
- lnadm:1006, lnrw:1007, lnsprov:1008, lnmtc:1009, lnro:1010
- mgcadm:1011, mgcrw:1012, mgcsprov:1013, mgcmtc:1014, mgcro:1015
- mgadm:1016, mgrw:1017, mgsprov:1018, mgmtc:1019, mgro:1020
- emsadm:1021, emsrw:1022, emssprov:1023, emsmtc:1024, emsro:1025

Below is a sample ldif file to add the “succssn” group:

```
dn: cn=succssn,ou=group,dc=labnet,dc=us
dc=nortel,dc=com,o=internet
changetype: add
cn:succssn
gidnumber: 105
memberuid: kcaudill
memberuid: ferreira
objectclass: top
objectclass: posixGroup
```

Note: Consult your LDAP server manual for information on loading data into the directory server.

c Add users to the LDAP server, and associate them to user groups.

Below is a sample ldif file to add a user:

```
dn: uid=kcaudill,ou=people,dc=us,dc=nortel,dc=com
cn: kelly Caudill
givename: Kelly
sn: Caudill
gidnumber: 105
homedirectory: /tmp
uidnmuber: 10002
ojectclass: top
ojectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: posixaccount
objectclas: account
ojbectclass: shadowwaccount
uid: kcaudill
shadowlastchange: 6445
loginshell: /bin/ksh
gecos: Kelly Caudill
userpassword: mypassword
```

Note: Consult your LDAP server manual for information on loading data into the directory server.

At your workstation

4 Telnet to the Integrated EMS server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS central security server on which you want to change the PAM

5 When prompted, enter your user ID and password.

6 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

7 When prompted, enter the root password.

8 Save a backup copy of “nsswitch.conf”, which is located in the “/etc” directory.

9

> **ATTENTION**
> This step can reconfigure “nsswitch.conf”, therefore, ensure you saved a backup copy of “nsswitch.conf” before you proceed.

Configure the Solaris Native LDAP client using the “ldapclient” command.

Note: Information on the “ldapclient” command, is available at the following link: http://docs.sun.com/db?q=ldap+configuration+guide&p=doc%2F806-5580

10 Replace “nsswitch.conf” with the backup copy of “nsswitch.conf”.

11 Update the “/etc/nsswitch.conf” file as follows:

a Add “ldap” as the first option for the password and group.

The entries would look similar to “passwd: ldap files” and “‘group: ldap files” after the change.

This enables the group information to come from LDAP.

12 Edit the /etc/pam.conf file as follows:

a Add pam_ldap with sufficient setting as the first entry in the pam.conf” file as indicated:

- change “login auth” to “ login auth sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “other auth” to “other auth sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “sesm auth” to “sesm auth sufficient /usr/lib/security/$ISA//pam_ldap.so.1 try_first_pass”
- change “secclient auth” to “secclient auth sufficient /usr/lib/security/$ISA//pam_ldap.so.1”

b Add pam_ldap with sufficient setting as the first entry in the pam.conf” file as indicated:

- change “login account” to “login account sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “other account” to “other account sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “sesm account” to “sesm account sufficient /usr/lib/security/$ISA//pam_ldap.so.1 try_first_pass”
- change “secclient account” to “secclient account sufficient /usr/lib/security/$ISA//pam_ldap.so.1”

c Add pam_ldap with sufficient setting as the first entry in the pam.conf” file as indicated:

- change “other session” to “other session sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “sesm session” to “sesm session sufficient /usr/lib/security/$ISA//pam_ldap.so.1 try_first_pass”
- change “secclient session” to “secclient session sufficient /usr/lib/security/$ISA//pam_ldap.so.1”

d Add pam_ldap with sufficient setting as the first entry in the pam.conf” file as indicated:

- change “other password” to “other password sufficient /usr/lib/security/$ISA//pam_ldap.so.1”
- change “sesm password” to “sesm password sufficient /usr/lib/security/$ISA//pam_ldap.so.1 try_first_pass”
- change “secclient password” to “secclient password sufficient /usr/lib/security/$ISA//pam_ldap.so.1”

13 You have completed this procedure.

Note: When the LDAP authentication mechanism is selected, you must use the UNIX passwd command with the “-r” option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “`passwd -r file <userid>`”.

Reverting the client server to its previous configuration

Application

Use this procedure if you configured an SSPFS-based central security client to use the Integrated Element Management System (EMS) central security server, but want to revert to its previous configuration, which is not to use the Integrated EMS central security server.

Prerequisites

To perform this procedure, you need to have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to change the authentication mechanism

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Configure PAM as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

select -
```

b Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

d Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

 x - exit

select -
```

e Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 x - exit

select -
```

f Enter the number next to the “pam_orig” option in the menu.

Example response

```
===Executing “pam_orig”

Switching to original PAM configuration

Enter “ok” to continue
Enter anything else to exit
```

g Accept to switch to the original PAM configuration by typing

ok

and pressing the Enter key.

Example response

```
Stopping pam_radius

Deconfiguring pam_radius

===”pam_orig” completed successfully
```

h Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

6 Re-provision the user accounts in Unix. In a two-server configuration, re-provision the user accounts on the active server first and then on the inactive server. If required, refer to procedure Setting up local user accounts on a Sun server.

7 You have completed this procedure.

Configuring the security server SunONE component

Application

Use this procedure to configure the security server SunONE component if you want it to run in secure mode on the central security server and central security clients.

Use one of the methods below according to your office configuration:

- Simplex configuration (one server) on page 116
- High-availability configuration (two servers) on page 118

Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (EMS) server. If required, refer to procedure Installing an HTTPS certificate on an SSPFS-based server on page 121.

> ***Note:*** In a two-server configuration, the HTTPS certificate must be installed on both servers (active and inactive).

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Integrated EMS server on which you want to configure the security SunONE component

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Reconfigure the SunONE IS client environment on the system to use SSL as follows:

a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/
current_s1isext/swmgmt/bin
```

and pressing the Enter key.

> ***Note:*** The above command is entered on one line.

b Execute the configuration script by typing

```
# ./configure_sspfs_s1isext.sh -ssl
```

and pressing the Enter key.

The above command reconfigures the SunONE IS client environment on the central security server to use SSL.

6 Restart the Web Server as follows:

a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

7 Restart the Web Services as follows:

a Stop Web services by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start Web Services by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

8 Restart the Radius server as follows:

a Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.

b Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.

9 You have completed this procedure.

High-availability configuration (two servers)

At your workstation

1 Telnet to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Active Integrated EMS server on which you want to configure the security SunONE component

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Reconfigure the SunONE IS client environment on the Active server to use SSL as follows:

a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/
current_s1isext/swmgmt/bin
```

and pressing the Enter key.

Note: The above command is entered on one line.

b Execute the configuration script by typing

```
# ./configure_sspfs_s1isext.sh -ssl
```

and pressing the Enter key.

The above command reconfigures the SunONE IS client environment on the Active central security server to use SSL.

6 Initiate a failover by typing

```
# shutdown -i 0 -y
```

and pressing the Enter key.

7 Reconfigure the SunONE IS client environment on the newly Active server to use SSL as follows:

a Change directory to the configuration script by typing

```
# cd /opt/nortel/applications/security/
current_s1isext/swmgmt/bin
```

and pressing the Enter key.

Note: The above command is entered on one line.

b Execute the configuration script by typing

```
# ./configure_sspfs_s1isext.sh -ssl
```

and pressing the Enter key.

The above command reconfigures the SunONE IS client environment on the Active central security server to use SSL.

8 Restart the Web Server on the newly Active server as follows:

a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

9 Restart the Radius server on the newly Active server as follows:

a Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.

b Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.

10 Restart Web Services on the newly Active server as follows:

a Stop Web services by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start Web Services by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

11 You have completed this procedure.

Installing an HTTPS certificate on an SSPFS-based server

Application

Use this procedure to install an HTTPS certificate on a Succession Server Platform Foundation Software (SSPFS)-based server. An HTTPS certificate enables secure transmission of communications, and is required from the SN07 release onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see Types of certificates below).

> **ATTENTION**
> An HTTPS certificate is preserved over an SSPFS upgrade. Therefore, you do not need to perform this procedure following an SSPFS upgrade if an HTTPS certificate was already installed on the server.

Types of certificates

Following, are the three types of security certificates that can be used. These certificates differ in the level of trust that needs to be assigned to a server.

- a certificate granted from a well known certificate authority (CA): used when the server is used in a public way, such as for e-commerce websites
- a company-generated certificate: used when the server is used internally, and the operating company has its own internal CA
- a self-signed certificate created locally on the server: used when the server is used in a more restricted manner.

  Note: When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers “yes”, the server can be accessed. If the user answers “no”, nothing further will be received from the server.

Use one of the methods below to install the certificate according to your office configuration:

- Simplex configuration (one server)
- High-availability configuration (two servers)

Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in the ATM/IP Solution-level Configuration Management document, NN10409-500.
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

  Note: The name of the certificate should match the host name of the server. Nortel Networks recommends the installation of a unique certificate for each host. A separate file contains the key, and should not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories “ssl.crt” and “ssl.key” must already exist in the “/opt/apache/conf” directory.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

5 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Example response:

```
You are about to be asked to enter information
that will be incorporated into your
certificate request.
What you are about to enter is what is called
a Distringuished Name or a DN.
There are quite a few fields but you can leave
some blank.
For some fields there will be a default value.
If you enter ‘.’,the field will be left blank.
------

Country Name (2 letter code) [AU]:
```

d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)
[Some-State]:
```

e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet
Widgits Pty Ltd]:
```

g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

h When prompted, enter the name of the department that owns the server.

Example response:

```
Common Name (eg, YOUR name []:
```

i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

```
Email Address []:
```

j When prompted, enter the email address of the organization that owns the server.

6 Place the certificate file (server.crt) you obtained in “/opt/apache/conf/ssl.crt”.

Note: If directory “ssl.crt” does not exist, you need to create it.

7 Place the key file (server.key) you obtained in “/opt/apache/conf/ssl.key”.

Note: If directory “ssl.key” does not exist, you need to create it.

8 Change the certificate's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

9 Change the key file's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

12 Restart the WEBSERVER as follows:

a Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

13 Restart the WEBSERVICES as follows:

a Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

14 If the CS2M software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure "Configuring the SESM server application" in the ATM/IP Solution-level Configuration Management document, NN10409-500.

15 If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

16 You have completed this procedure.

High-availability configuration (two servers)

At your workstation

1 Telnet to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Active server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

If you are	Do
using a self-signed certificate	step 5
not using a self-signed certificate	step 6

5 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Example response:

```
You are about to be asked to enter information
that will be incorporated into your
certificate request.
What you are about to enter is what is called
a Distringuished Name or a DN.
There are quite a few fields but you can leave
some blank.
For some fields there will be a default value.
If you enter ‘.’,the field will be left blank.
------

Country Name (2 letter code) [AU]:
```

d When prompted, enter a two letter code for the country where the server is located.

Example response:

```
State or Province Name (full name)
[Some-State]:
```

e When prompted, enter the full name of the State or Province where the server is located.

Example response:

```
Locality Name (eg, city) []:
```

f When prompted, enter the city where the server is located.

Example response:

```
Organization Name (eg, company) [Internet
Widgits Pty Ltd]:
```

g When prompted, enter the name of the company that owns the server.

Example response:

```
Organizational Unit Name (eg, section) []:
```

h When prompted, enter the name of the department that owns the server.

Example response:

```
Common Name (eg, YOUR name []:
```

i When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

```
Email Address []:
```

j When prompted, enter the email address of the organization that owns the server.

6 Place the certificate file (server.crt) you obtained in "/opt/apache/conf/ssl.crt".

Note: If directory "ssl.crt" does not exist, you need to create it.

7 Place the key file (server.key) in"/opt/apache/conf/ssl.key".

Note: If directory "ssl.key" does not exist, you need to create it.

8 Change the certificate's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

9 Change the key file's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

10 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

11 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

12 Restart the WEBSERVER as follows:

a Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

b Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

13 Restart the WEBSERVICES as follows:

a Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

b Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

14 If the CS2M software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure “Configuring the SESM server application” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

15 Clone the image of the node with the HTTPS certificate onto the other node using procedure *Cloning the image of one node in a cluster to the other node* in ATM/IP Solution-level Security and Administration, NN10402-600.

16 If you installed an HTTPS certificate on an existing SSPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

17 You have completed this procedure.

Setting up local user accounts on a Sun server

Application

Use this procedure to add local user accounts on a Sun server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups (see User groups).

ATTENTION
If upgrading from a release prior to (I)SN06, existing users must be assigned to primary group “succssn” for login access, and to one or more Secondary user groups to specify the operations the user is authorized to perform (see step 13 of this procedure).

If you choose to centrally manage your user accounts, refer to procedure “Adding new users”.

User groups

Users of the Nortel Networks OAM&P client applications must belong to the primary user group “succssn” for login access. Users must also belong to one or more secondary user groups listed in the table below, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the table below.

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel Networks OAM&P client applications. The user group operations are listed in the table below.

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

- Node provisioning operations
- Carrier provisioning operations
- Audit operations
- Alarm operations
- Internet transparency operations
- Trunk provisioning operations
- Trunk maintenance operations
- ADSL provisioning operations
- Line provisioning operations
- Line maintenance operations
- V5.2 provisioning operations
- Patching operations

Node provisioning operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x

Node provisioning operations

	User group				
Command	**mgcadm**	**mgcrw**	**mgcmtc**	**mgcsprov**	**mgcro**
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			

Node provisioning operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

	User group				
Command	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

	User group				
Command	**emsadm**	**emsrw**	**emsmtc**	**emssprov**	**emsro**
View/filter alarms					x

Internet transparency operations

	User group				
Command	**mgcadm**	**mgcrw**	**mgcmtc**	**mgcsprov**	**mgcro**
Query NAT					x
Query media proxy					x
Change associated NAT		x			

Trunk provisioning operations

	User group				
Command	**trkadm**	**trkrw**	**trkmtc**	**trksprov**	**trkro**
Get tuple					x
Get tuple range					x
Get CM CLLI					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			
List all tuples	x				
Suspend application	x				
Restore application	x				

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set CM CLLI			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

	User group				
Command	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

	User group				
Command	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwIp					x

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5Ring)					x					x
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, audit, restart, and image from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group “succssn” by typing

```
# useradd -g succssn <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups) and any other user groups you noted in step 12 to which the user already belonged (include comma between groups, but no space)

userid
is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

Note: The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

14 You have completed this procedure.

Deleting local user accounts from a Sun server

Action

Use this procedure to delete local user accounts from a Sun server.

If you are centrally managing your user accounts, refer to procedure “Deleting users”.

> **ATTENTION**
> User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5

ATTENTION

DO NOT delete the following critical user IDs from the server:

root, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, oracle

Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

6 You have completed this procedure.

Managing user sessions on the Security Token Administration GUI

Integrated EMS Security Token Administration GUI can be used to:

- view user session (or token) information
- terminate user sessions

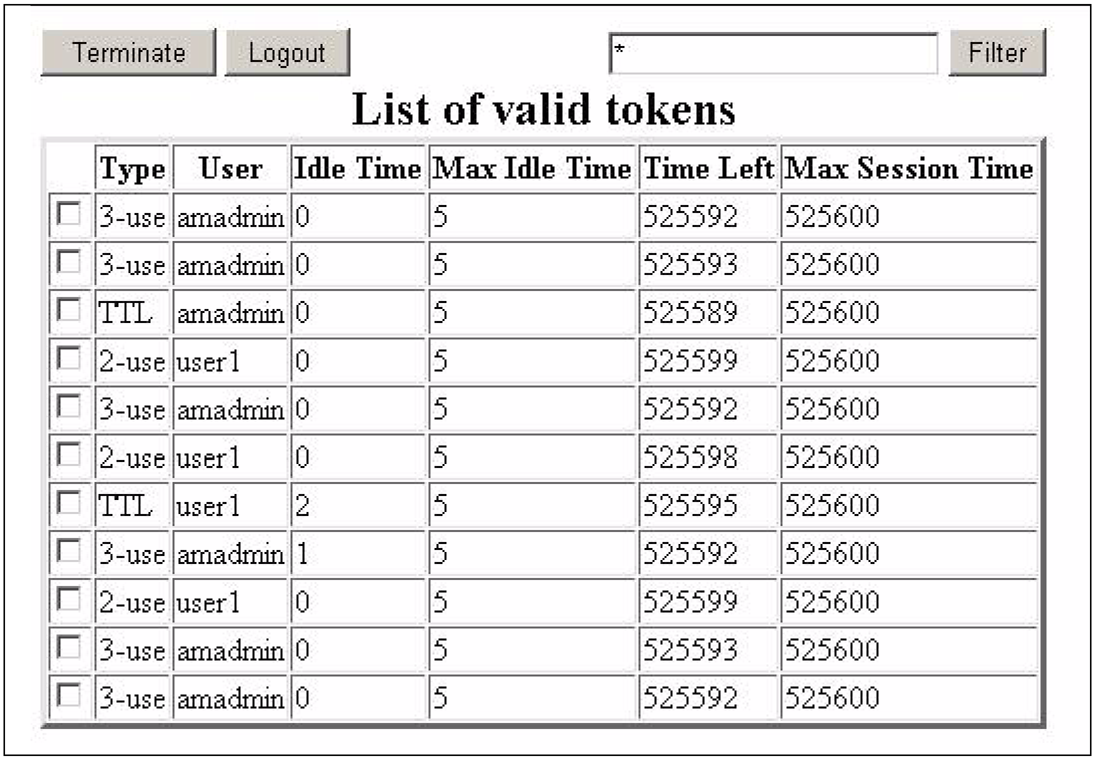
Integrated EMS Security Token Admininstration GUI displays all of the user sessions that are available to the Identity Server and displays the expiration time for each session. See List of valid tokens window.

Integrated EMS Security Token Administration GUI displays the following:

- the user sessions that are available
- the amount of time (minutes) remaining for a user session
- the maximum time (minutes) before the session expires after which the user session must re authenticate to regain access
- the time (minutes) that have expired while the user session is idle
- the maximum time (minutes) that a user session can remain idle

For details on how to log in to the Integrated EMS Security Token Administration GUI, see Launching the Integrated EMS Security Token Administration GUI.

List of valid tokens window



*

List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
☐	3-use	amadmin	0	5	525592	525600
☐	3-use	amadmin	0	5	525593	525600
☐	TTL	amadmin	0	5	525589	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525592	525600
☐	2-use	user1	0	5	525598	525600
☐	TTL	user1	2	5	525595	525600
☐	3-use	amadmin	1	5	525592	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525593	525600
☐	3-use	amadmin	0	5	525592	525600

Launching the Integrated EMS Security Token Administration GUI

Use this procedure to launch the Integrated EMS Security Token Administration GUI.

Prerequisites

To perform this procedure, the user account you are using to log into the Integrated EMS Security Token Administration GUI must be set up on the Integrated EMS server and have administration privileges.

To verify that the user account is set up, see the procedure for Listing all users.

Action

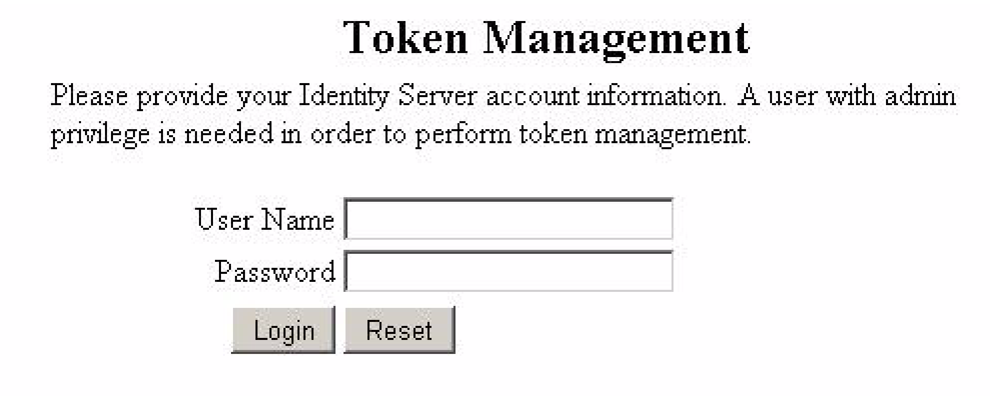
At a web browser

1 Launch the Integrated EMS Security Token Administration GUI using a URL in the format of:

```
http://hostname:8080/tokenadmin
```

The Token Management window is displayed as in the following figure.

Token Management window



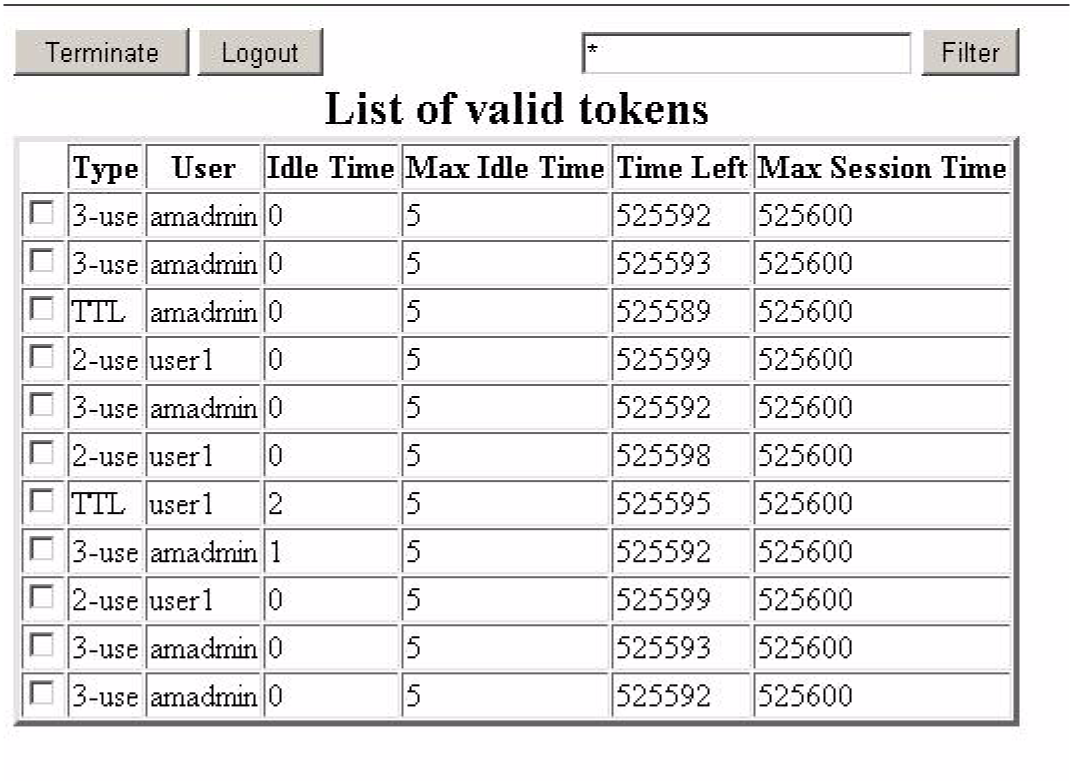
Token Management

Please provide your Identity Server account information. A user with admin privilege is needed in order to perform token management.

2 Enter your user name in the User Name field.

3 Enter your password in the Password field.

4 Click Login. The List of valid tokens window opens.



List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
□	3-use	amadmin	0	5	525592	525600
□	3-use	amadmin	0	5	525593	525600
□	TTL	amadmin	0	5	525589	525600
□	2-use	user1	0	5	525599	525600
□	3-use	amadmin	0	5	525592	525600
□	2-use	user1	0	5	525598	525600
□	TTL	user1	2	5	525595	525600
□	3-use	amadmin	1	5	525592	525600
□	2-use	user1	0	5	525599	525600
□	3-use	amadmin	0	5	525593	525600
□	3-use	amadmin	0	5	525592	525600

Terminating a user session

Use this procedure to terminate a user session.

Prerequisites

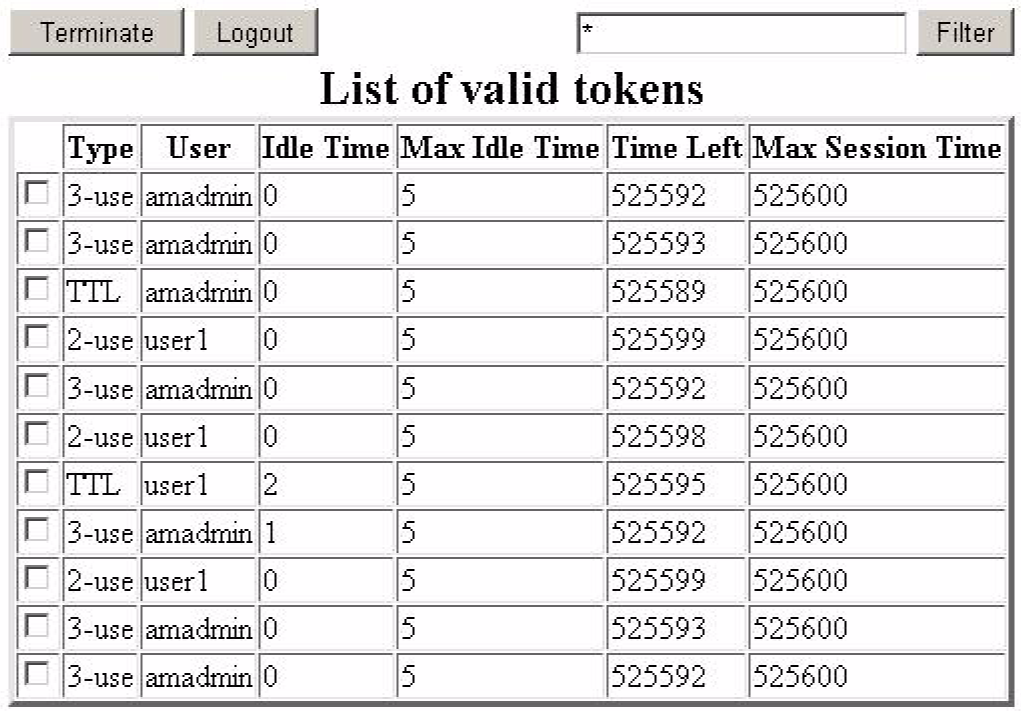
You require a user account with administration privileges to perform this task.

Action

At the Integrated EMS Security Token Administration GUI

1 Log in to the Integrated EMS Security Token Admininstration GUI.

- **a** Open the Token Management dialog box. See Launching the Integrated EMS Security Token Administration GUI.
- **b** Enter your user name in the User Name field.
- **c** Enter your password in the Password field.
- **d** Click Login. The List of valid tokens window opens.



List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
□	3-use	amadmin	0	5	525592	525600
□	3-use	amadmin	0	5	525593	525600
□	TTL	amadmin	0	5	525589	525600
□	2-use	user1	0	5	525599	525600
□	3-use	amadmin	0	5	525592	525600
□	2-use	user1	0	5	525598	525600
□	TTL	user1	2	5	525595	525600
□	3-use	amadmin	1	5	525592	525600
□	2-use	user1	0	5	525599	525600
□	3-use	amadmin	0	5	525593	525600
□	3-use	amadmin	0	5	525592	525600

2 Select the appropriate check boxes to select the sessions that you want to terminate.

3 Click Terminate Session.

The List of valid tokens window is updated with the list of valid tokens.

Viewing a user session

Use this procedure to view one user session or a range of sessions that are available to the Identity Server.

Prerequisites

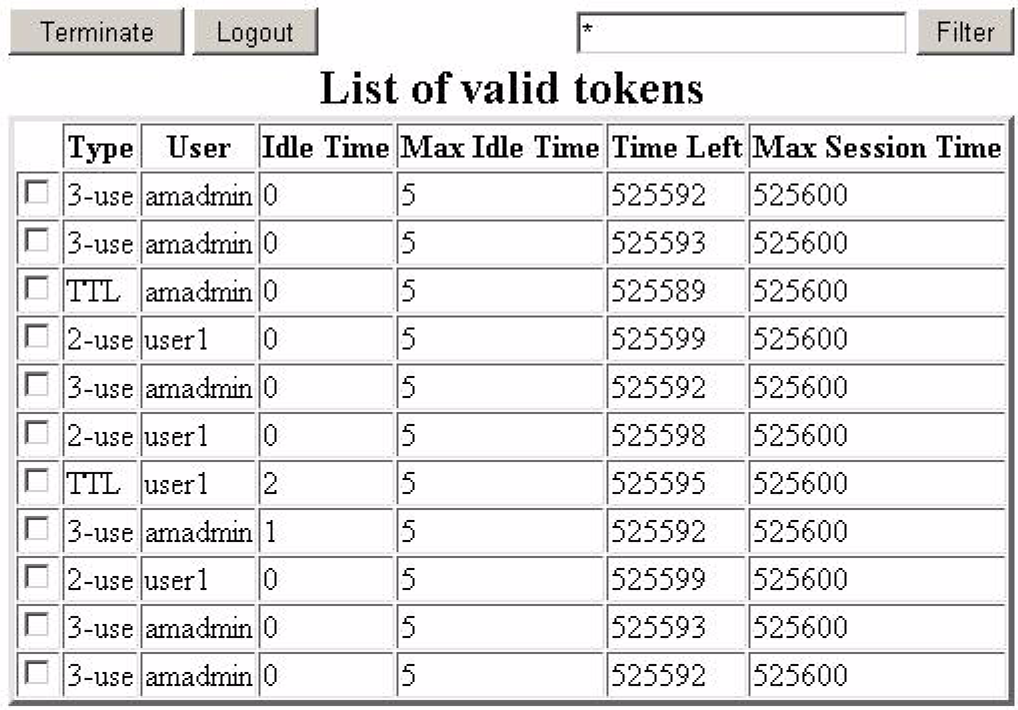
You require a user account with admininstration privileges to perform this task.

Action

At the Integrated EMS Security Token Administration GUI

1 Log in to the Integrated EMS Security Token Admininstration GUI.

- **a** Open the Token Management window. See Launching the Integrated EMS Security Token Administration GUI.
- **b** Enter your user name in the User Name field.
- **c** Enter your password in the Password field.
- **d** Click Login. The List of valid tokens window opens.



List of valid tokens

	Type	User	Idle Time	Max Idle Time	Time Left	Max Session Time
☐	3-use	amadmin	0	5	525592	525600
☐	3-use	amadmin	0	5	525593	525600
☐	TTL	amadmin	0	5	525589	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525592	525600
☐	2-use	user1	0	5	525598	525600
☐	TTL	user1	2	5	525595	525600
☐	3-use	amadmin	1	5	525592	525600
☐	2-use	user1	0	5	525599	525600
☐	3-use	amadmin	0	5	525593	525600
☐	3-use	amadmin	0	5	525592	525600

2 Enter a string in the Filter field.

Note: You can enter any character in the Filter field, including a meta-character (*).

Example
To list all users whose names start with am, enter am*.

To list all users whose names end with min, enter *min.

To list all users whose names contain ad, enter *ad*.

3 Click Filter to refresh the List of valid tokens window and view the list of valid tokens using the value in the Filter field.

Configuring DCE on a Sun server

Application

Use this procedure to configure the Distributed Computing Environment (DCE) on a Sun server following a Succession Server Platform Foundation Software (SSPFS) upgrade. Only perform this procedure if DCE is used as an authentication mechanism. As of (I)SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

Prerequisites

This procedure has the following prerequisites:

- unconfigure DCE if DCE was configured prior to upgrading the SSPFS - refer to procedure Configuring DCE on a Sun server, if required
- obtain the following information
  - — the DCE cell name for your customer-provided DCE cell

    Note: This should be the same DCE cell that contains the core manager.

  - — the host name or IP address of the DCE Master Security Server (MSS)
  - — the host name or IP address of the DCE Cell Directory Server (CDS)
  - — the DCE cell administrator password.
  - — the host name or IP address of the DCE Time Server (DTS)

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that uses DCE as an authentication method

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View

 2 - Configuration

 3 - Other


 X - exit

select -
```

6 Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

7 Enter the number next to the “DCE Configuration” option in the menu.

Example response

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>

 2 - dce_unconf <Unconfigure the DCE Client>


 X - exit

select -
```

8 Enter the number next to the “dce-conf” option in the menu.

Example response

```
DCE Cell Name(default:)
```

9 Enter the DCE Cell Name.

Example response

```
Master Security Server Name(default:)
```

10 Enter the host name or IP address of the MSS.

Example response

```
Time Server Name(default:)
```

11 Enter the host name or IP address of the DTS.

Example response

```
CDS Server Name(default:)
```

12 Enter the host name or IP address of the CDS

Example response

```
You have selected to configure your DCE
environment as the following:

Host Name                         : znc0s0jx

DCE Cell Name                     :
rtpptm.sdm.nortel.com

Time Server Name                  : wnc0s0j8

Master Security Server Host Name : wnc0s0j8

CDS Server Host Name              : wnc0s0j8

Continue with configuration?(default:Y[Y/N]
```

13 Continue the configuration by typing

y

and pressing the Enter key.

Example response

```
Synchronizing time with wnc0s0j8......

Tue Apr 16 15:00:47 2002

done synchronizing time with wnc0s0j8(0)

Configuring DCE..............................

Default DCE configuration timeout value
successfully changed.

Gathering current configuration information...

Enter password for principal cell_admin:
```

14 Enter the cell administrator password and press the Enter key.

Example response

```
Configuration of DCE Host, znc0s0jx, will now
begin.

Configuring RPC...

Starting RPC...

RPC was started successfully.

RPC configuration is complete.

Configuring the Security client...

Information from the /etc/krb5.conf.backup file
may need to be manually merged into the
/etc/krb5.conf file.

Starting the Security client...

The Security client was started successfully.

Security client configuration is complete.

Configuring the Directory client...

Starting the Directory client...

Waiting up to 10 minutes for the directory
server.

Contacted the directory server.

The Directory client was started successfully.
```

```
Waiting up to 10 minutes for DCED registration
to be functional.
Directory client configuration is complete.
Configuring the DTS client...
Starting the DTS client...
The DTS client was started successfully.
DTS client configuration is complete.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State  Running State
Security client      Configured          Running
RPC                  Configured          Running
Directory client     Configured          Running
DTS client           Configured          Running

The component summary is complete.
Configuration of DCE Host, znc0s0jx, was
successful.
Configuration completed successfully.
done configuring DCE
Gathering current configuration information...
Configuration of DCE Host, znc0s0jx, will now
begin.
There are no components in the request that need
to be configured.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State  Running State
Security client      Configured          Running
RPC                  Configured          Running
Directory client     Configured          Running
```

```
DTS client          Configured          Running
```

```
The component summary is complete.

Configuration of DCE Host, znc0s0jx, was
successful.

Configuration completed successfully.

=== “dce_conf” completed successfully
```

15 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

16 You have completed this procedure.

Configuring the Single Sign-On token

Application

Use this procedure to configure the values for the Single Sign-On (SSO) token and view the current SSO values. The SSO values are the time the Single Sign-On (SSO) token can remain idle before it becomes invalid, and the time the SSO token id can be used before it expires.

The SSO capability enables users to access multiple network elements, applications, and features from a single login session.

Prerequisites

You need root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to configure SSO

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View

 2 - Configuration

 3 - Other


 X - exit

select -
```

6 Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

7 Enter the number next to the “Succession Element Configuration” option in the menu.

Example response

```
Succession Element Configuration
 1 - RADSVR Application Configuration
 2 - S1IS Application Configuration
 3 - RESMON Application Configuration
 4 - NPM Application Configuration
 5 - PSE Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

8 Enter the number next to the “S1IS Application Configuration” option in the menu.

Example response

```
S1IS Application Configuration
 1 - LIST_TOKEN_VALUES (List the current session
     and idle times set in Sun One.)
 2 - TOKEN_ADMIN (Change the token idle and
      session expiry time)


 X - exit

select -
```

If you want to	Do
view the current SSO values	step 9
configure SSO values	step 10

9 Enter the number next to the “LIST_TOKEN_VALUES” option in the menu.

Example response

```
=== Executing “LIST_TOKEN_VALUES”

30 # Idle time of the token
365  # Session time of the token

=== “LIST_TOKEN_VALUES” completed successfully
```

If you	Do
want to re-configure SSO values	step 10
do not want to re-configure SSO values	you have completed this procedure

10 Enter the number next to the “TOKEN_ADMIN” option in the menu.

Example response

```
=== Executing “TOKEN_ADMIN”

Enter the new Token Idle Time:
```

11 When prompted, enter the desired value for the idle time of the SSO token, which is the time the token can remain idle before it becomes invalid. The default value is 30 minutes.

```
Enter the new Token Session Time:
```

Example response

12 When prompted, enter the desired value for the duration of the SSO token id, which is the time the token id can be used before it expires. The default value is 525600 minutes (365 days).

Example response

```
Enter the new Token Idle Time:60
Enter the new Token Session Time: 182
Success 0: Successfully completed.
NOTE: Operation succeeded.

=== “TOKEN_ADMIN” completed successfully
```

13 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

14 You have completed this procedure.

Integrated EMS server startup options

This section describes the procedures for starting and shutting down the Integrated EMS Server. After starting the Integrated EMS Server successfully, connect the client with the Integrated EMS Server. The following sections give the details:

- Starting the Integrated EMS server
- Shutting down the Integrated EMS server
- Viewing the Integrated EMS server status
- Starting Integrated EMS server in HTTPS mode

Starting the Integrated EMS server

This section describes how to start the Integrated EMS Server using the servman from the system where Integrated EMS Server is installed.

To start the Integrated EMS Server, follow these steps:

At Integrated EMS Server system

1 Telnet or switch to the host in which Integrated EMS Server is running.

2 Execute the following command to start the Integrated EMS Server.

```
/opt/servman/bin/servstart IEMS
```

Servman starts the Integrated EMS with the following message.

```
Starting IEMS through servstart
IEMS Started
```

The following table lists the ports occupied for various processes by Integrated EMS Server.

Ports occupied by various processes in Integrated EMS server

Process	Port Occupied	Communication	Communication data transfer direction
Integrated EMS Server (same as Web Server)	9090(default)	HTTP	Both incoming and outgoing
Integrated EMS Server HTTPS mode	9091	SSL	Both incoming and outgoing
Trap port	162(default)	UDP	Both incoming and outgoing (only if an “Inform” message is received)
TFTP	69(default)	UDP	Both incoming and outgoing
Servlet Engine (Tomcat) port	18009 (default)	UDP	Both incoming and outgoing

Ports occupied by various processes in Integrated EMS server

Process	Port Occupied	Communication	Communication data transfer direction
Agent port	8001 (default)	UDP	Both incoming and outgoing
Client Server Communication port [Primary]	9004	TCP	Both incoming and outgoing
Client Server Communication port [Secondary]	9005	TCP	Both incoming and outgoing
Web Container	18005	TCP	Both incoming and outgoing
Tomcat Shutdown	18009	TCP	Both incoming and outgoing

Note: The ports listed in the preceding table are for the Integrated EMS Client connected to the Integrated EMS Server directly or Integrated EMS Clients residing behind Firewalls.

Shutting down the Integrated EMS server

Integrated EMS Server shutdown process shuts down all the sub-processes and properly releases all the system resources. The shutdown process must be properly executed to ensure that the system does not leave any operation incomplete, or the database information in an inconsistent state.

The following sequence of operations takes place during the Integrated EMS Server shutdown process:

1. Stop all the schedulers.
2. Notify the registered shutdown observers.
3. Shut down all the sub-processes (sub-modules), which execute specific tasks.
4. Disconnect all database connections.
5. Shut down the web server (if started by Integrated EMS).
6. Exit (the main process).

To shut down the Integrated EMS Server, kill the related Java application shell by pressing the Ctrl+C (Control) key.

The shutdown process checks for the authenticity and the permissions of the user invoking the shutdown operation, and is allowed only if the user has the proper permissions.

Shutting down the Integrated EMS server through the command line

The server can be shut down using the servman. To shutdown the server using the servman, switch command line and type the following command and press Enter key.

```
/opt/servman/bin/servstop IEMS
```

Servman stops the Integrated EMS Server with the following message

```
Stopping group using servstop

The I-EMS Server on host “192.168.4.176” was
successfully shutdown

IEMS Stopped
```

Viewing the Integrated EMS server status

This section describes the procedure to check the Integrated EMS Server status using the servman from the system where Integrated EMS Server is installed.

To check the Integrated EMS Server status, follow these steps:

At Integrated EMS Server workstation

1 Telnet or switch to the host in which Integrated EMS Server is running.

2 Execute the following command to start the Integrated EMS Server.

```
/opt/servman/bin/servquery -status -g IEMS
```

If the Integrated EMS Server is running, the following message is displayed.

```
IEMS Instance is UP
```

If the Integrated EMS Server is not running, the following message is displayed.

```
IEMS Instance is DOWN
```

Starting Integrated EMS server in HTTPS mode

HTTPS is the secure mode of communication between the client and the server of Integrated EMS.This mode of communication is also known as the Secured Socket Layer (SSL)mode. Data transmitted in this mode is encrypted over the TCP or IP connection and can be viewed through browsers.To view the secured data through the browsers, the “https” (instead of “http”) protocol must be specified in the URL.

Integrated EMS Web Start client can be connected to the server through the HTTPs 9091 port.

To enable or disable HTTPS mode of communication for Integrated EMS, follow these steps:

At Integrated EMS server

1. Connect to the host in which Integrated EMS Server is installed with telnet session.
2. Switch to the <IEMS Home>/bin folder.
3. Run the script SSLUtil.sh with the parameter “Enable” or “Disable”. Use “Enable” parameter to enable the HTTPS mode for Integrated EMS Server and use “Disable” option to disable the HTTPS mode.

   Example

   To enable HTTPS mode for Integrated EMS Server, run the script using “Enable” parameter as given in the following example.

   ```
   # SSLUtil.sh Enable
   ```

   Example

   To disable HTTPS mode for Integrated EMS Server, run the script using “Disable” parameter as given in the following example.

   ```
   # SSLUtil.sh Disable
   ```

Using jobs

Using jobs in Integrated EMS, the Integrated EMS administrator can execute a task or set of tasks at a specified time based on a set of specified conditions. Jobs are tasks that are executed by Integrated EMS at a system level, at a specified time. Jobs are used to control a variety of network activities, such as automated backups, routing and prioritizing the network traffic, bandwidth allocation, cleaning up database tables, deleting failed nodes, and so on. Jobs are displayed in the Jobs panel under the Administration Tools node in the Integrated EMS tree. This section describe jobs and job operations under the following headings:

- Adding and modifying jobs
- Other job operations
- Using the alarms clearing job
- Using the table cleanup job
- Using the DB cleanup job

Adding and modifying jobs

Jobs can be added or modified using the corresponding menu commands displayed for the Jobs panel (under the Administration Tools node) of the Integrated EMS. An added job is displayed in the Jobs panel and its details are stored in the database. Once a job is added, it remains in the *enabled* state until it is changed to any other state such as execute, suspend, or disable.This section deals with Adding and Modifying Jobs.

To add a job, follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree

3 Select the **Job-->Add Job** menu command to add a job.

4 Specify a name for the added job in the **Instance Name** textfield.

5 Click **Add** button to open the **IEMS Performance Metrics Collection Job Details** dialog.

To specify details for Collection,Transfer and Report Jobs, refer to the following sections of the Integrated EMS Performance Management, NN10327-711.

1.Collection Job: Working with Data Collection Jobs

2.Transfer Job: Adding Transfer Job

3.Report Job: Adding Report Job

For details of alarm clearing, table cleanUp and DB cleanup jobs, refer to the following sections:

1.Using the alarms clearing job

2. Using the table cleanup job

3. Using the DB cleanup job

To modify an existing job, follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

3 Select the job to be modified from the Jobs panel.The screen displays the Jobs panel, listing all the current Jobs.

4 Select the **Edit-->Modify Job** menu command to modify the existing job.

The modified details of the job are displayed in the **Object Properties** dialog. The modified details are also stored in the database. Refer to the sections mentioned for **Adding Jobs**, to view the respective job details displayed in the GUI.

5 Click **OK** button to apply the modifications of the job.

Other job operations

In general, the word job refers to a plan of action. In Integrated EMS, job refers to executing a task or set of tasks at a specified time based on a set of specified conditions. Jobs are tasks that are executed by Integrated EMS at a system level, at a specified time. In Integrated EMS, Jobs are used to control a variety of network activities such as automated backups, routing, and prioritizing the network traffic, bandwidth allocation, cleaning up database tables, deleting failed nodes.

This job framework enables administration of the Integrated EMS Server and the network elements managed by it. The primary goal of the job engine is to simplify the administration of complex functions. In Integrated EMS, Jobs are used to customize the behavior of the Integrated EMS and to provide a framework for adding jobs for different network elements.

Integrated EMS jobs can be broadly classified into two categories:

- **Periodic Jobs**: Jobs are triggered periodically by the server after specified time interval. By default, the periodic Jobs are configured to be executed at interval of 10 seconds.
- **Non-periodic Jobs**: Jobs are executed at a specified time. There is no fixed time interval and you must specify the time at which the Job is to be executed. No default value is assigned for non-periodic Jobs.

Searching jobs

To search for a job, follow these steps:

At the Integrated EMS workstation

1. Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).
2. Select the **Job-->Search** menu command from the menu bar.The **Policy Search Dialog** is displayed.
3. Specify the criteria and click **Execute Query**. The jobs matching your criteria are displayed in the Jobs panel.
4. To view all the jobs again, click **Select all Jobs** in the Search dialog.

Enabling jobs

By default, a job is enabled once its added. Any operation can be performed on a job only when it is enabled.To enable a job in the GUI follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Double click the job displayed in the **Jobs** panel or select the **Edit-->Modify Job** menu command in the menu bar.

3 Choose the status as **Enable** in the displayed form.

> ***Note:*** Similarly, *disable* the job status by choosing the corresponding option in the displayed form. Once a job is disabled, it must be manually *enabled* as it remains in the *disabled* state even after restarting the server.

4 Click OK button to apply the modifications of the job.

Executing jobs

To execute a job, follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

3 Select the job to be executed from the Jobs panel.

The screen displays the Jobs panel, listing all the current Jobs.

4 Select the **Edit-->Execute Job** menu command to execute the job.

Suspending jobs

Suspend job can be used to stop an executing job temporarily at

runtime. To suspend a job follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Client (refer to the “Launching Integrated EMS Java Web Start Client” of *Integrated EMS Basics, NN10329-111*).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

3 Select the job to be suspended in Jobs panel.

4 Choose the **Edit-->Suspend Job** command to suspend the job.

Note: An “Info” event is generated on suspending the job, which is displayed in the Network Events browser. The details of the event is:

```
Index - <index>
Message - <message>
Category - <others>
Source - <servname or IP>-IEMS
Date/Time - <date/time>
Log Number - 540
Event Type - OFFL
Log Name - EMJS
Event Label - OM Collection Job Status
Office Identifier - COM4

Body Text -

Location: <Serv Name>
JobInstance: <Job name>
State: Suspended
Date/Time: <date/time>
Equip Identifier -<serv name>
Severity - Info
Component ID -<IEMS=<serv name>, Software=<collection job
name>>
```

5 Click **Yes** button to suspend the job.

Note: If a job is to be suspended permanently, then select Disable in the status field of the dialog, which opens when you double click the jobs in the Jobs panel.

Removing jobs

To delete a job, follow these steps:

At the Integrated EMS workstation

1 Launch the Integrated EMS Client (refer to the “Launching Integrated EMS Java Web Start Client” of *Integrated EMS Basics, NN10329-111*).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

3 Select the job to be deleted in Jobs panel.

4 Choose the **Edit-->Delete Job** command to delete the job.

Understanding colors in jobs

Every job displayed in the Jobs panel is highlighted with a color, which indicates the status of the Job.

The following table lists the default color schemes for the Jobs, and the corresponding status:

Significance of Colors for Jobs

Color	Significance
Yellow	Stopped job
Green	Job which is being executed
Cyan	Executed job
Grey	Disabled job
Orange	Suspended Job

Using the alarms clearing job

The alarms clearing job allows the Integrated EMS administrator to clear the alarms manually from the devices that have not intimated the status for a specified period. This ensures that the alarms table does not continue to increase in size with every change of device state each day. This job specifies how many days the alarms can remain in a non-cleared state. If this job is not used, the Integrated EMS administrator must clear the alarms that are in a non-cleared state for a specified period. By default, the job is enabled and is displayed in the *Jobs* panel of Integrated EMS client.

To use the alarms clearing job in the Jobs panel, follow these steps:

At Integrated EMS workstation

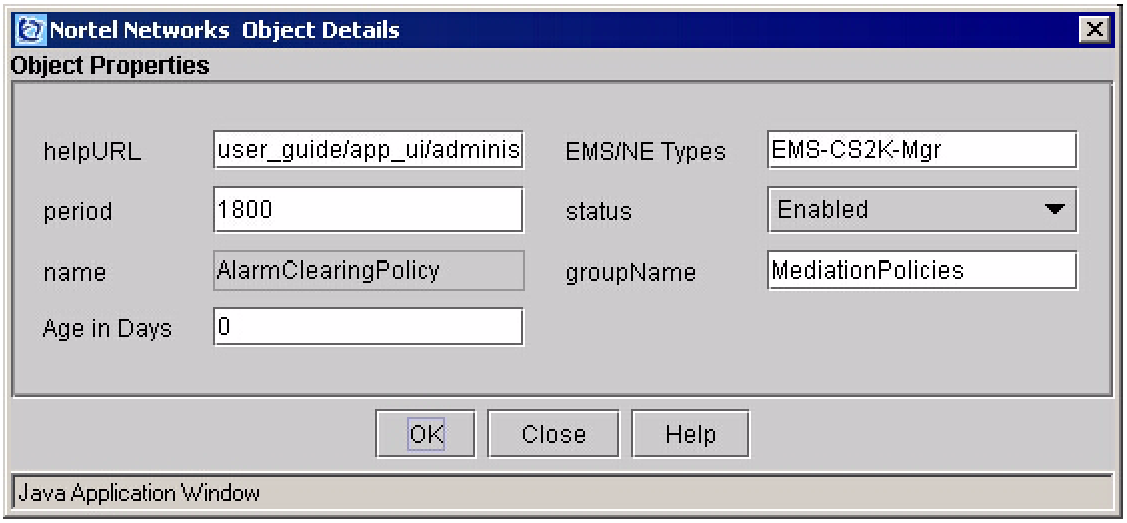
1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

The Jobs Panel is in the right-hand side of the window, with the list of jobs tabulated.

3 Select the Job named **AlarmClearingPolicy** and double-click it.

This opens the Object Details window, as shown in the following figure.



Nortel Networks Object Details

Object Properties

helpURL	user_guide/app_ui/adminis	EMS/NE Types	EMS-CS2K-Mgr
period	1800	status	Enabled
name	AlarmClearingPolicy	groupName	MediationPolicies
Age in Days	0		

The following table gives the description and use of each field in the Object Details window. Change the details as required and click the *OK* button to update the job.

Description of properties in the object details window for an alarm clearing job

Property	Description
helpURL	This field must not be changed. It simply points to the corresponding help file.
EMS/NE Types	This field specifies the type of EMS/NE to which the job applies. Several EMS/NE types can be specified separated with commas.
period	This field indicates the period in seconds. This field must not be changed.
status	The status can either be enabled or disabled. If the administrator chooses to disable a certain job, the operator is unable to schedule, start, or stop the execution of a job.
name	This field indicates the name of the job.
groupName	This is a grouping field that helps you to organize the jobs. Enter any required value. This field can later be used to query for the matching jobs to organize the different jobs.
Age in Days	This field specifies the age of alarms (in days) to be cleared when the job is executed.

> ***Note:*** You can execute a Job only if it is enabled.To check whether the Job is enabled, refer to the “Other job operations“.
>
> If a Job is running and its status is changed to disabled, the job execution is stopped. After the job status is reverted to enabled state, execute the job using, Edit-->Execute Job menu command.

After updating a job (and if the job status is enabled), execute the job using the menu command Edit-->Execute Job.

Using the table cleanup job

The Table cleanup job enables the Integrated EMS administrator to clean up manually “performance data” from the database after the specified period. For definition of “performance data”, refer to the “List of Terms and Abbreviations”of I*ntegrated EMS Performance Management, NN10327-711*. This ensures that the data table does not continue to increase in size with every addition of data collected each day. By default, this job is enabled and is displayed in the *Jobs* panel of Integrated EMS client.

To use the Table cleanup job in the Jobs panel, follow these steps:

At the Integrated EMS workstation

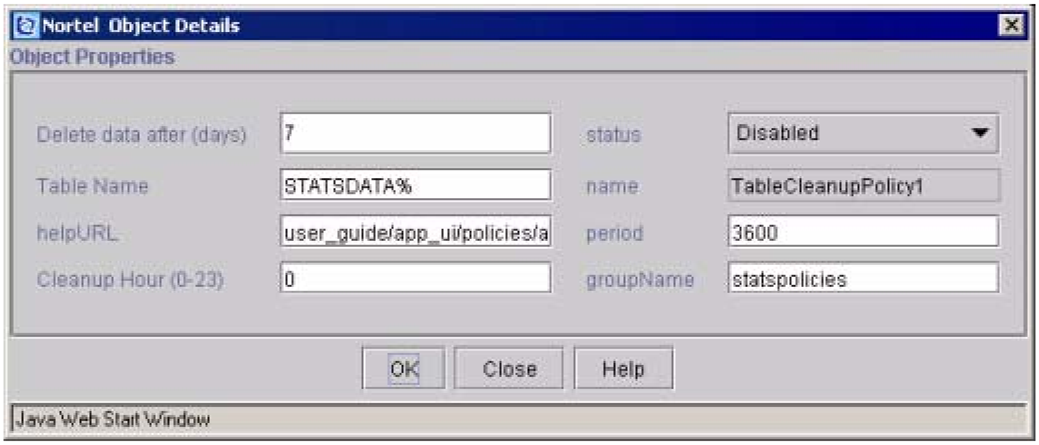
1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

The Jobs panel is in the right-hand side of the window, with the list of jobs tabulated.

3 Select the Job named **TableCleanupPolicy1** from the table and double-click it.

This opens the Object Details window, as shown in the following figure.



Delete data after (days)	7	status	Disabled
Table Name	STATSDATA%	name	TableCleanupPolicy1
helpURL	user_guide/app_ui/policies/a	period	3600
Cleanup Hour (0-23)	0	groupName	statspolicies

The following table gives a description of each field in the Object Details window for the TableCleanupPolicy1 job. Change the details required and click the *OK* button to update the job.

Description of properties in the object details window for a table cleanup job

Property	Description
Delete data after (days)	The number of days after which the data must be removed.
Status	The status can either be enabled or disabled. If the administrator chooses to disable a certain job, the operator is unable to schedule, start, or stop the execution of a job
Table Name	This field indicates the name of the table for which the job applies. You can change the table name if required. As data contained in the STATSDATA table is cleaned up by the policy, you can specify any “STATSDATA_<date of table creation>” in this field.
Name	This field indicates the name of the job.
helpURL	This field must not be changed. It simply points to the corresponding help file.
period	This field indicates the time period after which the job is executed, automatically. This field must not be changed.
Cleanup Hour	This specifies when to clean up the statistics (hour of the day). The cleanup can happen at any time during the hour; the time with in the hour cannot be controlled. The default value is 0, that is, done between 12 midnight and 1 a.m.
groupName	This is a grouping field that helps you to organize the jobs. Enter any required value. This field can later be used to query for the matching jobs to organize the different jobs.

Note: You can execute a job if the job status is enabled. To check whether the job is enabled, refer to “Other job operations“.

If a job is running and its status is changed to *Disabled*, then the job execution is stopped. Only after the job status is reverted to *Enabled*, you can execute the job using **Edit-->Execute Job**.

Once a job is updated(and is in enabled state), execute the Job using the menu command **Edit->Execute Job**.

Using the DB cleanup job

The DB cleanup job monitors the tablespace size of Integrated EMS, periodically and generates an alarm when the tablespace size exceeds a given threshold value. The threshold value (in percentage) of the tablespace size and the time period (in seconds) for monitoring it, can be set manually through the GUI. By default, the DB cleanup job is enabled and can be viewed in the Jobs panel under the **Administrative Tools** node of Integrated EMS client. The job requires to be executed to initiate the monitoring of the tablespace size.

To use the DBCleanup job in the Jobs panel, follow these steps:

At the Integrated EMS workstation

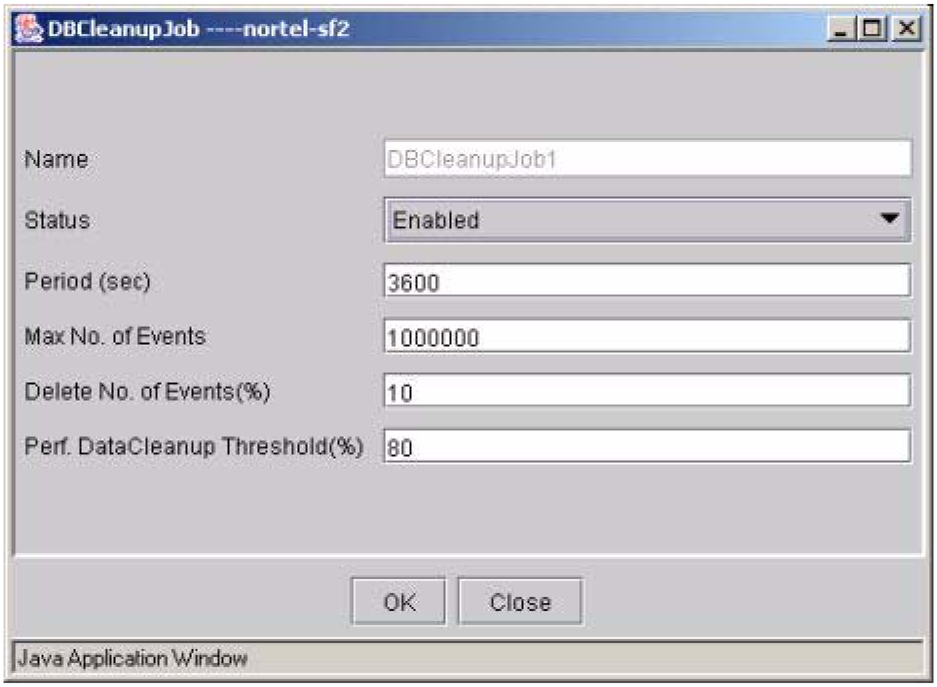
1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Jobs** node under the Administrative Tools node in the Integrated EMS tree.

The Jobs Panel is in the right-hand side of the window, with the list of jobs tabulated.

3 Select the Job named **DBCleanupJob** from the table and double-click it.

This opens the DBCleanupJob details window, as shown in the following figure.



Name: DBCleanupJob1
Status: Enabled
Period (sec): 3600
Max No. of Events: 1000000
Delete No. of Events(%): 10
Perf. DataCleanup Threshold(%): 80

The following table gives a description of each field in the DBCleanupJob details window for the same job. Modify the details required and click the “OK” button to update the job.

Description of Properties in DBCleanupJob window

Property	Description
Name	This field indicates the name of the job.
Status	This field indicates the status of the job. By default, the status is “Enabled”. The “Disabled” option can be chosen when the job is to be disabled.
Period (sec)	This field indicates the time period interval (in seconds) for executing the job, automatically.The default time period is 3600 seconds.
Max No. of Events	This field indicates the maximum number of events that are configured for the Events tablespace. On exceeding the configured value an event (EMJS 606) is generated.

Description of Properties in DBCleanupJob window

Property	Description
Delete No. of Events(%)	This field indicates the number (in percentage) of events to be deleted from the events table on exceeding the configured value (of **Max No.of Events** field). As per the value (in percentage) specified, the number of events are deleted during execution of the DB cleanup job.
Perf. DataCleanup Threshold(%)	This field indicates the threshold (in percentage) value for the performance data tablespace. On exceeding the threshold value, an event is generated and the data is deleted by the DB cleanup job.

Note: You can execute a Job only if the Job status is enabled. To check whether the Job is enabled, refer to "Other job operations".

If a job is running and its status is changed to *Disabled*, then the job execution is stopped. Only after the job status is reverted to *Enabled*, you can execute the job using **Edit-->Execute Job**.

Once a job is updated (and is in enabled state), execute it using the menu command **Edit-->Execute Job**.

Configuring tablespace size

The **Configure Tablespace** tool accessed from *iems_config.sh* tool (located in the <IEMS Home>/bin directory) can be used for configuring the database tablespace size. This tool can be used for querying the tablespace size, extending the tablespace size and for reducing the tablespace size.

Querying tablespace size

To query the tablespace size, follow these steps:

At the Integrated EMS server

1 Run the iems_config.sh file located in <IEMS Home>/bin directory.

2 The following list of options are displayed.

```
1 Configure OfficeName
2 Configure TableSpace
X Exit
```

3 Type “2” and press Enter key to select the **Configure TableSpace** option.

```
1 Configure OfficeName

2 Configure TableSpace

X Exit

2
```

4 The list of tablespace that can be configured are as follows:

1. IEMS_TS
2. IEMS_EVENT_TS

X. Exit

5 Choose the tablespace from the given list.

```
1 IEMS_TS

2 IEMS_EVENT_TS

X EXIT

Choose a tablespace to proceed:
```

6 Based on the chosen tablespace, the following list of options are displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size
      x to Exit
```

7 Choose “q” to select *Query IEMS tablespace size*. Integrated EMS tablespace size is displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size
      x to Exit

Choose an Option:q

The <table name>tablespace size - 2000.0 MB.
Do you want to continue?
```

8 Choosing to continue again displays the list of options.

Extending tablespace size

To extend the tablespace size, follow these steps:

At the Integrated EMS server

1 Run the iems_config.sh file located in <IEMS Home>/bin directory.

2 The following list of options are displayed.

```
1 Configure OfficeName

2 Configure TableSpace

X Exit
```

3 The list of tablespace that can be configured are as follows:

1. IEMS_TS
2. IEMS_EVENT_TS

X. Exit

4 Choose the tablespace from the given list.

```
1 IEMS_TS

2 IEMS_EVENT_TS

X EXIT

Choose a tablespace to proceed:
```

5 Based on the chosen tablespace, the following list of options are displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size
      x to Exit
```

6 Choose “e” to select *Extend IEMS tablespace size*. Integrated EMS tablespace size is displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size

      x to Exit

Choose an Option:e

Warning: You are attempting to modify the
tablespace size.
Do you want to continue?
```

7 On choosing to continue, you need to enter the value by which the tablespace is to be extended. An example value is given here.

```
Do you want to continue?

Yes(y) No(n)y
Enter the size (in MB)to be increased- 10
The tablespace size is extended to 2010 MB.

Do you want to continue?
```

8 Choosing to continue again displays the list of options.

Reducing tablespace size

To reduce the tablespace size, follow these steps:

At the Integrated EMS server

1 Run the iems_config.sh file located in <IEMS Home>/bin directory.

2 The following list of options are displayed.

```
1 Configure OfficeName

2 Configure TableSpace

X Exit
```

3 The list of tablespace that can be configured are as follows:

1. IEMS_TS
2. IEMS_EVENT_TS

X. Exit

4 Choose the table space from the given list.

```
1 IEMS_TS

2 IEMS_EVENT_TS

X EXIT

Choose a tablespace to proceed:
```

5 Based on the chosen tablespace, the following list of options are displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size
      x to Exit
```

6 Choose “r” to select *Reduce IEMS tablespace size*. Integrated EMS tablespace size is displayed.

```
Press q to Query <table name> tablespace size
       e to Extend <table name> tablespace size
       r to Reduce <table name> tablespace size
      x to Exit
```

```
Choose an Option:r
```

```
Warning: You are attempting to modify the
tablespace size.
Do you want to continue?
```

7 On choosing to continue, you need to enter the value by which the tablespace is to be reduced. An example value is given here.

```
Do you want to continue?
```

```
Yes(y) No(n)y
Current size is - 2005
```

```
Enter the size(in MB)to be decreased - 19
```

```
The tablespace is reduced to 1986 MB.
```

```
Do you want to continue?
```

8 Choosing to continue again displays the list of options.

Administering fault operations

Integrated EMS administrator can configure the event filter, alarm filter, and event cleanup interval. In addition, the administrator can change the attributes for SNMP fault feeds. This section explains these functions under following headings:

- Configuring event filters
- Configuring alarm filters
- Configuring the destination for SNMP traps
- Configuring the Event Cleanup interval
- Changing attributes for SNMP fault feeds

Configuring event filters

Event filters are configured to facilitate initiation of actions for the selected events automatically. This section explains in detail the procedure to configure event filter and event filter actions.

Defining an Event filter involves the following steps:

- Selecting the Events for which necessary action has to be initiated
  - Specifying the Match Criteria - Source, (Failure)Entity, Category, Severity, and others.
- Specifying the Actions to be taken for Events that match the criteria.
  - Sending an E-mail, Sending a Notification.

This section explains the following tasks:

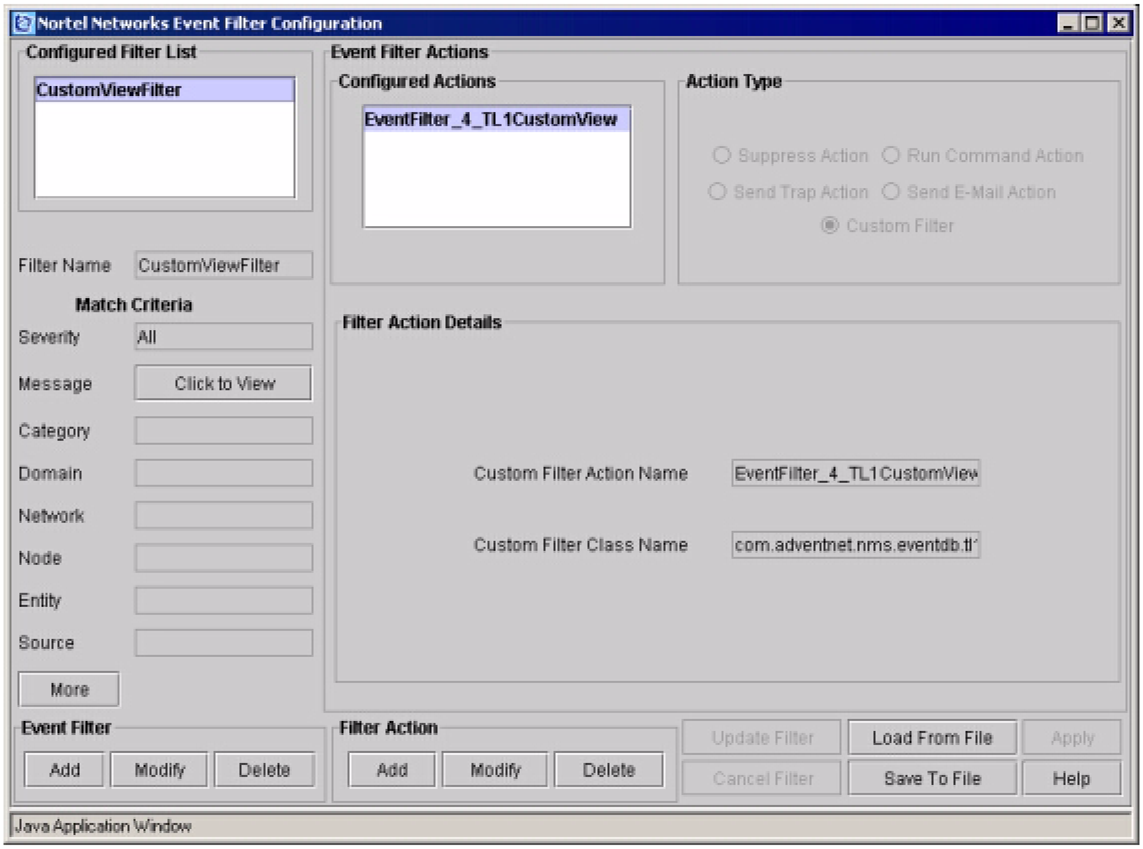
- Use of event filters
- Dynamic Configuration from Integrated EMS Client
- Setting the match
- Configuring event filter actions
- Enable/Disable event filters

When an event is raised, you may need to execute certain actions. Integrated EMS provides you the event filters to perform automatic actions, such as sending an e-mail, suppressing the event, generating traps, on the occurrence of an event. You can also execute some classes (Custom Filter Action), when there is a generation of an event

Using the Event Filter Configuration interface

To invoke the Event Filter configuration User Interface, follow these steps:

1. Refer the “Invoking Integrated EMS Java Web Start Client” to invoke the Integrated EMS Client.
2. Select the **Network Events** node under the Fault Management node in Integrated EMS client.
3. Choose the **Edit-->Configure-->Event Filters** menu command to invoke the Event Filter Configuration user interface similar to the shown screen shot.



Nortel Networks Event Filter Configuration

Configured Filter List: CustomViewFilter

Configured Actions: EventFilter_4_TL1CustomView

Action Type: ● Custom Filter

Filter Name: CustomViewFilter

Match Criteria

Severity: All

Custom Filter Action Name: EventFilter_4_TL1CustomViev

Custom Filter Class Name: com.adventnet.nms.eventdb.tl1

Using various options in the event filter

There are various options available with event filters. When you are configuring for the first time, you can choose the “Add” option to configure the event filter. Later depending on the requirement, you can choose any of the other options available with event filters. Following are the options available with event filters.

- Adding Event Filters and Associating Actions to them
- Modifying Event Filter and Filter Actions
- Load From File
- Save To File
- Re-Ordering Event Filters and Filter Actions

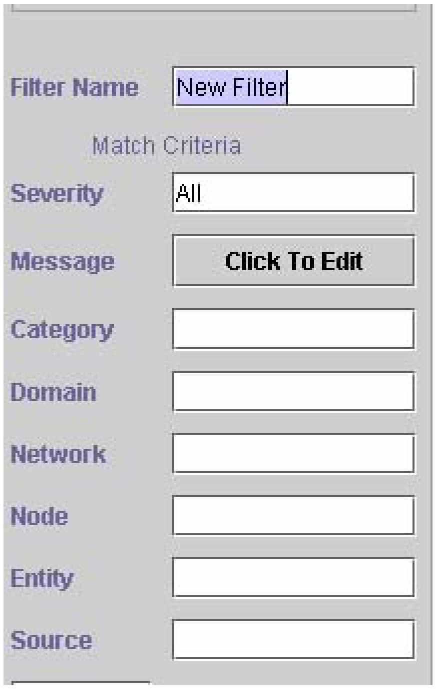
Adding event filters and associating actions to them

To add an event filter, choose “Add” Option from the Event Filter frame that is displayed at the bottom of the form, just below the “More” Option. The next step involves the following:

- Setting the Event filter parameters and Setting the match criteria for identifying the Event for which the event filter has to be applied.
- Configuring the Event filter actions
- Configuring Event Filters List

Setting the event filter parameters

When the Add button is clicked, the fields in the Event Filter parameters gets enabled. The following image shows a partial view of the Event Filter form, showing the editable Event Filter parameters.



Filter Name: New Filter

Match Criteria

Severity: All

The description of the Event Filter parameters is provided below. All other parameters, except Filter Name, are used to configure the match criteria.

- Filter Name - This field denotes the name of the filter.This is useful to choose a filter, when multiple filters are managed.

Match criteria

- Severity - This field specifies the match criteria based on the severity of the event, such as Critical, Major.
- Message - The message specified in this field is matched with the message of the incoming event, such as Interface failure, Status Poll failed.
- Category - This is a property of the event object which cannot hold a category name to which the event belongs. This is used for better organization of events.Example, communication, other, environmental.
- Domain - This is a property of the event object which cannot hold any domain-specific information.The information may either be based upon the physical location, functional or logical categorization of the source of the event. The domain name of the event can be specified to display events of a particular domain.Example,
- Network - This property can hold the information about the network to which the source of the event belongs. Using this criteria, events belonging to a particular network can be displayed.Example, 198.162.4.0
- Node - This field holds any additional information about the source of the event. Event filters can be specified for events that have the name of the node as specified in this field. Example, for an event originating device “IEMS-Mgr” the node can provide additional information such as “Sam-CS2K-Mgr”.
- Entity - This field stores information about the exact device in which the problem has occurred. They are unique identification string for the non info events.
- Source - This property holds the information about the source of the event. Events matching a source can be filtered out using this field. Example, IEMS-Mgr, abc-CS2K-Mgr

Setting match criteria

The match criteria determines whether the incoming event must be filtered or not. If this field is left blank, it is automatically matched. The condition for the event filter to be applied is that all the match criteria specified must be satisfied. Even if one criterion fails, the filter is not be applied.

The following expressions can be used, while specifying the match criteria.

- Wildcard - Asterisk (*): This is used to signify a match of 0 or more characters of any value. For example, “Failed*” is matched with any string starting with “Failed”.
- Negation - Exclamation (!): This can be used at the start of the field to specify exclusion of events matching this expression. For example, “!Failed” excludes the strings starting with “Failed”.
- Separator - Comma (,): Multiple values can be specified for a single search criteria by separating them with commas. For example, Critical, Major matches the string which is either Critical or Major.

To use the Event filter, enter the name of the event filter followed by its match criteria. You can also specify additional match criteria based on the properties of com.adventnet.nms.eventdb.Event object including User properties using the “More” option. While specifying the additional criteria, specify only those (the name of the event object is case-sensitive) properties that are in the event object. Apart from the default properties shown in the configuration wizard, you can add Event's base properties as match criteria such as, groupname, helpURL, id, and time in More option. Thus, More option serves for both Event's base properties as well as user properties.

Configuring event filter actions

To include a filter action, whenever the incoming event satisfies the match criteria, follow things these steps:

1. Click the **Add Action** button to add actions to the filter.
2. When the action type panel gets enabled, choose the type of action required and select it by clicking on the radio button.
3. The attributes corresponding to the selected action are to be displayed in the Filter Action Details panel.
4. Type in the relevant action details.
5. Click the **Update Action** button to add the action to the configured actions list. When this is done, the Update Action button changes to Update Filter button.

6. More actions can be added by using the Update Filter button. After keying in the actions, choose Update Filter button to add the filter to the configured event filter list.
7. At any time, you can choose Cancel Filter/Cancel Action option to abort adding the filter or actions.

> ***Note:*** An Event Filter without an action is not allowed. So, at least one action must be associated with an event filter.

You can configure event filters by setting the match criteria and specifying the actions to be executed, when an event matches the filter. The following types of event filter actions are supported in Integrated EMS:

- Suppress filter actions: These filter actions allow you to suppress events that match the filter criteria, either altogether or multiple events of the same type within a given interval.
- Send Trap actions: These filter actions allow you to send SNMP V1 traps for events matching particular filter criteria. The traps can be configured to have event data as specified by you. It can be configured to be sent to any desired host.
- Send E-mail actions: These filter actions allow you to send an e-mail for events matching particular filter criteria.
- Run command actions: These filter actions allow you to run a command on the server for events matching particular filter criteria. These can be used to send a page to someone, e-mail or any other desired command.
- Run your own Java class filter: You can write your own Java code to filter events and perform actions, and configure them to be applied for events matching particular filter criteria.

Configured Event Filter list

For a given event, all event filters in the event filters list are tested to see whether they satisfy the match criteria. If the event matches an Event filter, then the actions associated with that filter are executed. After the execution of the actions specified in the matching filter, the event is again checked with the remaining (subsequent) event filters on the list for any match. If a match is found, the corresponding event filter is executed. You can view the list of currently configured event filters in the Event Filters list. On choosing the event filter from the list, the corresponding filter details are displayed in the GUI.

> ***Note:*** There are separate Add, Modify, and Delete options available for Event Filter and Filter Action. The Update and Cancel options are common to both.

Modifying event filters and filter actions

In order to modify the existing event filters, select the event filter from the list and choose the **Modify Event Filter** option. Make the required changes and finally choose **Update Filter** option to confirm modification.

To modify the filter actions, select the filter action from the Action list and choose **Modify Action** option. Make the desired changes and finally choose **Update Action** option to confirm modification.

Deleting event filters and filter actions

To delete one or more event filters or filter actions, select the filters or actions from the list. Choose the **Delete** option or press the delete key to delete them.

Save to file

In order to reuse configured event filters and to have a backup of the configured event filters, so as to prevent loss of event filter information in the event manager, you can save them to a file. These can later be loaded into the same or another event manager. This provides a means of sharing event filter data with other users or one's customers.

To save the list of configured event filters, choose **Save to File** option. This opens a dialog where you can specify the filename to save the events filters on the server.

Load from file

This option is useful to load a set of event filters and add it to the existing list of event filters. To load the event filters, choose **Load From File** option. This brings up a dialog where you can specify the file on the server to load the event filters. Choose **Load** option to complete loading event filters from the specified file.

> ***Note:*** If you configure the event filters from the client and want the filters to take effect in the server immediately, click the **Apply** button. If they are not applied and the configuration window is closed, a dialog box pops up asking whether they need to be applied. Applying the event filter configuration to the server does not save the filters in persistent files. You must use the **Save To File** option to do so.

Reordering event filters and filter actions

You can reorder the Event Filters and Filter actions by drag and drop method. Drag the event filter or action and drop it into the desired position. Make use of the associated trap properties in an event filter, if the event is generated by a trap.

When an event is generated by a trap, the associated Trap PDU reference is maintained in the incoming event object, if the parameter TRANSIENT_TRAP_PDU_IN_EVENTunder the EventMgrmodule in NmsProcessesBE.conf file present in <IEMS Home>/conf directory is set to “true”. If the incoming event object has maintained the trap PDU reference, then you can make use of the properties of the trap, within the configured event filter. The properties of the trap cannot be used at the level of specifying match criteria (using the “More” option) and also for specifying values of the various action fields. The methodology of using the properties of the trap, using symbolic notations is similar as in Trap Parsers, except for the following differences:

- To access the values of the SNMP OID in the SNMP Variable bindings, the notation must start with% and not with $.
- All the special purpose tags must start with% instead and not with $.
- To access the SNMP OID in the SNMP Variable bindings, the notation must start with the same @.

Refer the table below for the different tags that cannot be used to access the various properties of the trap in event filter.

TAGS to Access the Properties of the Trap PDU

TAG Name	Description
%Agent	SNMP V1 Traps: If the device corresponding to the agent address, returned by the trap, has already been discovered by Integrated EMS, then this token fetches the name of the parent Managed object, corresponding to the interface object matching the agent address of the trap received. If the device corresponding to the agent address of the trap has not been discovered then this token returns the corresponding IP address of the agent address from which the trap has been received. Say for example, a trap is received from an agent and the corresponding device has already been discovered by Integrated EMS with the interface object being IF-webserver and the name of the parent managed object being webserver. In this scenario,%Agent returns webserver. In case the device is not yet discovered, then%Agent returns the IP address (192.168.1.30.). SNMP V2c & v3 Traps: If the device corresponding to the source address, contained by the trap received, has already been discovered by Integrated EMS, then this token fetches the name of the parent Managed object, corresponding to the interface object matching the source address of the received trap. If the device corresponding to the source address of the trap has not yet been discovered then this token returns the IP address of the Source of the Trap.
%Community	This token is replaced by the community string of the received trap.
%Enterprise	This token is replaced by the enterprise OID of the received trap. Applicable only to SNMP v1 traps, or else replaced with “”.
%GenericTyp e	This token is replaced by the generic type of the received trap. Applicable only to SNMP v1 traps, or else replaced with “”.
%Source	If the device corresponding to the source address, contained by the trap received, has already been discovered by Integrated EMS, then this token fetches the name of the parent Managed object, corresponding to the interface object matching the source address of the received trap. If the device corresponding to the source address of the trap received has not yet been discovered then the corresponding IP address of the source address is returned.
%SpecificTyp e	This token is replaced by the specific type of the received trap. Applicable only to SNMP v1 traps, or else replaced with “”

TAGS to Access the Properties of the Trap PDU

TAG Name	Description
%Uptime	This token is replaced by the uptime value in the received trap.
%TrapOID	This token is replaced by the trap OID of the received trap. Applicable only to SNMP v2C and v3 traps, or else replaced with “”
%*	This token is replaced by all the variable bindings (both OID and variable values) of the received trap. **Example** For the following varbinds, *2.2.1.1.221 INTEGER 30.1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10* the result is: ifIndex: 30, sysDescr: abc, ifIndex: 10
%#	This token is replaced by all the variable binding values (only variable values and not OIDs) of the received trap. **Example** For the following varbinds, *2.2.1.1.221 INTEGER 30.1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10* the result is: 30, abc, 10
%N	Here, N is a non-negative integer. This token is replaced by the (N+1)th SNMP variable value in the variable bindings of the received trap. The Index N starts from 0. **Example** For the following varbinds, *2.2.1.1.221 INTEGER 30.1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10* and for%1, the result is: abc
@*	This token is replaced by all the OID labels in the variable bindings of the received trap. **Example** For the following varbinds, *2.2.1.1.221 INTEGER 30.1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10* the result is: ifIndex: sysDescr: ifIndex

TAGS to Access the Properties of the Trap PDU

TAG Name	Description
@N	This token is replaced by the (N+1)th OID label in the variable bindings of the received trap. The index starts from 0. **Example** For the following varbinds, *2.2.1.1.221 INTEGER 30.1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10* and for @1, the result is: sysDescr
%IP-Source	This token is replaced by the IP address corresponding to the source address of the trap received, even if the object is not yet discovered by Integrated EMS.
%IP-Agent	This token is replaced by the IP address corresponding to the agent address of the trap received, even if the object is not yet discovered by Integrated EMS.

Enable or disable event filters

Event Filters can be enabled or disabled by using the parameter “enable” in the event.filters file present in <IEMS Home>/conf directory. This parameter can take two values, namely “true” or “false”. If the value is set to “true”, then the corresponding filter is enabled; and if it is set to “false”, it gets disabled.

```
<EVENT_FILTERS>
<FILTER
name=”MyEventFilter”
enable=”true”>
<FILTER_ACTIONclassName=”com.adventnet.nms.eventdb.User
Filter”
name=”userprop”
userclass=”com.adventnet.nms.eventdb.UserFilter” />
</FILTER>
</EVENT_FILTERS>
```

Note: The Enabling/Disabling of Event Filters can only be done by editing the event.filters file and not available through the Event Filter Configuration Interface.

Configuring alarm filters

Events are correlated into alarms.They represent the current status of the existing problems in a network. An Alarm Filter executes certain corrective actions whenever alarms are received with configurable matching criteria, such as suppressing multiple alerts in a given interval, running shell commands on the server system, sending e-mails, sending traps, and running custom code to filter alerts.

The processed alarms are stored in the database and can be viewed in the Alarm Viewer. The Alarm Viewer is asynchronously notified, as soon as the processing of an alert is completed.

An Alarm Filter can be configured using the Alert Filter Configuration tool. You can use the properties of an event object in certain text fields, such as Suppress Action, Run Command Action, Send Trap Action, and Send E-mail Action.

A Custom Filter can be created (at runtime) to enable more effective event correlation and fault management by adding application-specific rules when processing events and alarms.

The various ways of configuring alarm filters are as follows:

- Opening the Alert Filter Configuration tool
- Adding an alarm filter
- Action types
- Modifying alarm filters
- Saving alarm filter files
- Loading alarm filter files
- Reordering the configured alarm list
- Enabling and disabling alarm filters
- Deleting alarm filters
- Example of how to configure the system to send an email on alarm generation

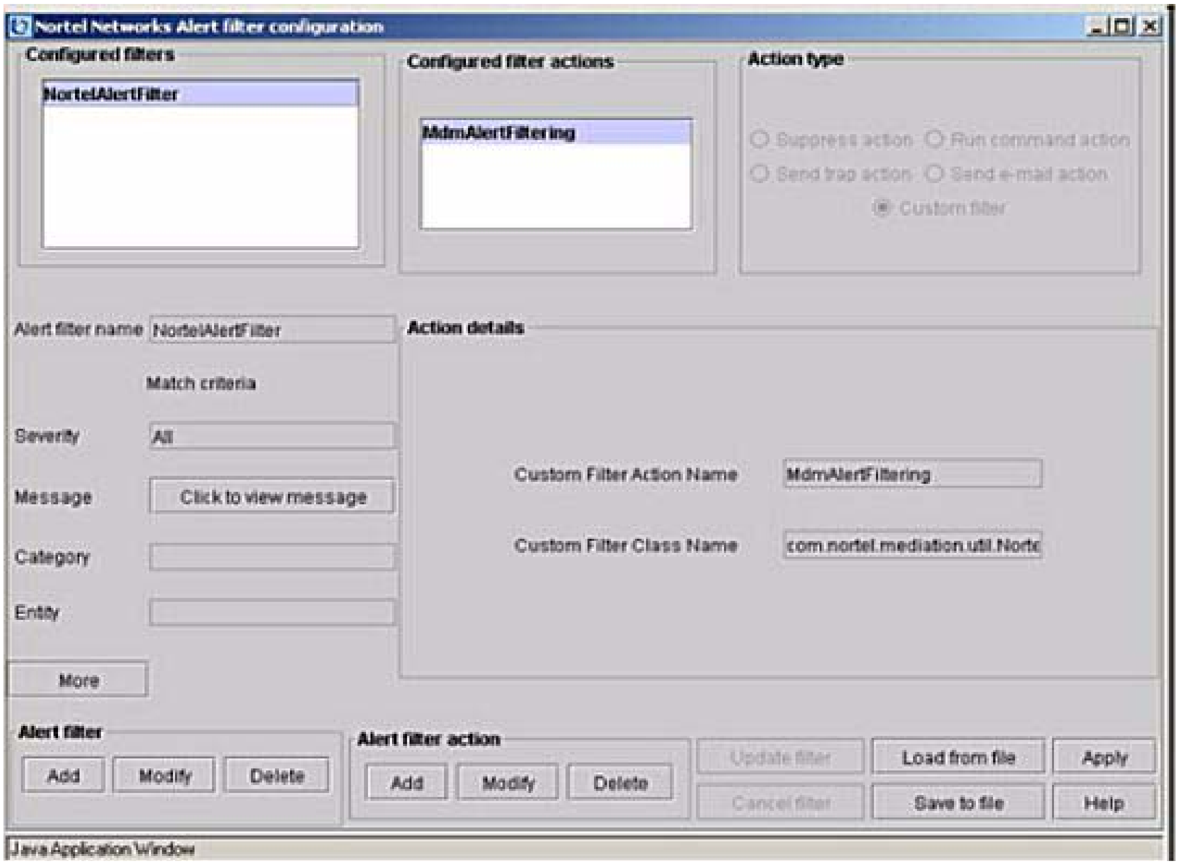
Opening the Alert Filter Configuration tool

The Alert Filters can be created or modified using the Alert Filter Configuration tool.

To open the Alert Filter Configuration tool

In Integrated EMS, click **Fault Management--> Alarms** node on the tree. From Edit menu, choose **Configure --> Alert Filters** or press Ctrl+Shift+A. Or

The Alert Filter Configuration tool is as shown below



Configured filters: NortelAlertFilter

Configured filter actions: MdmAlertFiltering

Action type: ○ Suppress action ○ Run command action ○ Send trap action ○ Send e-mail action ● Custom filter

Alert filter name: NortelAlertFilter

Severity: All

Category:

Entity:

Custom Filter Action Name: MdmAlertFiltering

Custom Filter Class Name: com.nortel.mediation.util.Norte

Adding an alarm filter

To add an alert filter

1 From the **Alert Filter Configuration** tool, click **Add** button in the **Alert filter** section of the tool GUI.

2 Specify a name for the Alarm Filter in the Filter Name field

3 Specify the appropriate values as Match Criteria. For information on each of the Match Criteria fields, refer to Match Criteria Table.

To specify additional match criteria for the Alarm Filter, click "More" button of the "Alarm Filter Configuration" tool GUI and execute the following steps:

4 On clicking **More**, the Alert Filter Configuration dialog box is displayed.

5 Specify the **Property Name** and **Match Criteria**. While specifying additional criteria, specify only those properties that are in the alarm object. The name must exactly match the case of the alarm object. You can also add alarm base properties as match criteria, such as group name, help URL, ID, and time.

6 To add more properties, click **More**.

7 Click **OK** after adding the properties.

To include filter action when an incoming alarm satisfies the match criteria, use the "Alert filter action" section of tool and execute the following steps:

8 Click **Add** button. The **Action type** fields are enabled.

9 Choose one of the actions from the Action types*. An Alarm Filter must have at least one action type associated with it.*

10 Specify values for the selected action.

11 Click **Update action** to add the action to the configured actions list. The Update Action button toggles to the Update Filter button.

12 To add more actions, click **Add** and specify values for the selected action. At any time, to abort the adding of Filter or Action, click **Cancel filter** and **Cancel action**, respectively.

Final Steps:

13 Click the **Update filter** button after adding the Alert Filter and its actions.

14 Click the **Save** button to save the configurations in the server.

Match Criteria Table

Field	Description
Severity	Match criteria based on the severity of the alarm, such as Critical, Major, and so on.
Message	Match criteria based on a message of the incoming alarm, such as Interface failure, Status Poll failed, and so on. Click the **Click to edit message**.The **Alert Filter Message** dialog box is displayed. Specify the message.
Category	Match criteria based on an alarm object property with a category name to which the alarm belongs. This is used to organize alarms.
Entity	Match criteria based on the information about an exact device in which a problem has occurred

The values that you specify in the Match Criteria determine whether the incoming alarm need to be filtered or not. If this field is left blank, it is matched, automatically. For the Alarm Filter to be applied, all the match criteria specified must be satisfied. If even one criterion fails, the Filter is not applied. For information on the expressions and combinations that can be used while specifying the match criteria, refer to the Configuring event filters.

Action types

The action types that can be configured for an Alarm Filter are:

- Suppress Action
- Run Command Action
- Send Trap Action
- Send Email Action
- Custom Filter

Configuring the alert filter actions

To include a filter action, whenever an incoming alarm satisfies the match criteria, follow these steps:

1. Click the **Add Action** button to add actions to the filter.
2. Once the **Action type** panel gets enabled, select the required action type by choosing the corresponding radio button.
3. The attributes corresponding to the selected action are to be displayed in the **Filter Action Details** panel.
4. Type in the relevant action details.
5. Click the **Update Action** button to add the action to the configured actions list. When this is done, the *Update Action* button changes to *Update Filter* button.
6. More actions can be added by using the *Update Filter* button. After keying in the actions, choose the *Update Filter* button to add the filter to the configured alert filter list.
7. At any time, you can choose *Cancel Filter/Cancel Action* option to abort adding the filter or actions.

Note: An alert filter must be associated with at least one action type.

You can configure alert filters by setting the match criteria and configuring the actions to be executed, when an alarm matches the filter criteria. Integrated EMS supports the following types of alert filter actions:

- Suppress filter actions: This filter action can be used to suppress or drop alarms that match the filter criteria. Either all the alarms are suppressed or alarms of the same type are suppressed within the given interval.The description of the fields to be filled in the Suppress filter action panel are as follows:

Field	Description
Suppress Action Name	This field is to specify a name for the suppress action type.
Suppress All	This field indicates whether the incoming alarms are to be suppressed or not. If you choose **Yes** then all subsequent alarms are suppressed. If you choose **No** then subsequent alarms generated within the specific time interval are suppressed.
Suppress Interval	This field is to specify the time interval (in seconds) to suppress the alarms. Here, except the first alarm which matches the criteria, all other subsequent alarms are suppressed in the configured time interval.

- Send Trap actions: The filter action can be used to send SNMP v1/v2c traps for alarms matching the filter criteria.The description of the fields to be filled in the Send Trap filter action panel are as follows:

Field	Description
Send Trap Action Name	This field is to specify a name for the filter action.
Trap Destination	This field is to specify the destination host to which the trap is to be sent.
Destination Port	This field is to specify the destination port to which the trap is to be sent.
Trap Community	This field is to specify the community for the trap to be sent.
Enterprise	This field is to specify the OID of the trap. This is only applicable for SNMP V1 traps alone.
Generic Type	This field is to specify the number to be used for the trap.This is only applicable for SNMP V1 traps alone.

Field	Description
Specific Type	This field is to specify the number to be used for the trap.This is only applicable for SNMP V1 traps alone.
SysUpTime(secs)	This field is to specify the sysuptime value to be used in the trap.
Variable Bindings List	Click **Add** in *Filter Action Details* panel to add Variable Bindings to the trap. **OID Value**: Specify the value of the Object ID. **SNMP Type**: Choose the appropriate SNMP string from the drop-down list. **Set Value**: Specify the set value associated with the selected SNMP type. Click **Update**. To add more Variable Bindings, click **Add** and specify the values.

- Send E-mail actions: This filter actions allow you to send an e-mail for alarms matching the filter criteria.The description of the fields to be filled in the Send E-mail filter action panel are as follows:

Field	Description
Send E-mail Action Name	This field is to specify a name for the filter action.
User Name	This field is to specify the user name using which the mail server authenticates you to send the email.
Password	This field is to specify the password using which the mail server authenticates you to send the email.
SMTP Server	This field is to specify the SMTP server address.
Recipient's Address	This field is to specify the destination address to which the e-mail is to be sent. More than one recipient can be addressed by using comma separator for the e-mail ids.
Sender's Address	This field is to specify the sender's address from which the e-mail is to be sent.

Field	Description
Subject	This field is to specify the subject of the mail.
Message	This field is to specify the message to be mailed.

- Run command actions: This filter action can be used to run a command on the server for alarms matching the filter criteria.It can be used to send a page, e-mail, or execute any other commands. The description of the fields to be filled in the Run Command filter action panel are as follows:

Field	Description
Run Command Action Name	This field is to specify a name for the filter action.
Run Command	This field is to specify the command that is to be executed. It must be ensured that the command is a machine executable program on the server that does not require a shell (it cannot be a batch file or a shell).For example, the command *dir* list all the directories available under< IEMS Home>.
Command Results	This field contains two options which can be chosen as per the requirement. **Append Output:** Check this check box if you want the output from the command to be appended to the alert message field. **Append Error**: Check this check box if you want the error from the command to be appended to the alert message field.
Abort After	This field is to specify the time after which the command execution is to be stopped.This field entry is important if you are appending the output or errors of the command to the alert message text.

- Custom filter: This filter can be used for configuring your customized filter classes to be invoked for alarms matching the filter criteria. The description of the fields to be filled in the Custom filter action panel are as follows:

Field	Description
Custom Filter Action Name	This field is to specify the name for the filter action.
Custom Filter Class Name	This field is to specify the custom filter's class name.

Modifying alarm filters

To modify the match criteria of Alert filters:

1 In the **Alert Filter Configuration** dialog box, select the Alarm Filter to be modified, from **Configured filters** list.

2 Click **Modify** in **Alert filter** section. All the fields in the Match criteria section are enabled.

3 To specify your own properties to the alarm object generated by the Alarm Filter, click **More**. The **Alert Filter Configuration** dialog box is displayed.

Specify the name and value of the property in Property Name and Match Criteria fields, respectively. To specify more properties, click More. When you are finished adding values and properties, click OK

4 Make appropriate changes and click **Update filter**.

5 To apply this configuration to the server, click **Apply**.

To modify the match criteria of Alert filter action

6 In the **Alert Filter Configuration** dialog box, select the Alert Filter to be modified, from **Configured filters** list. Its corresponding actions are listed in **Configured filter** actions section.

7 Select the action.

8 Click **Modify** in **Alert filter action** section. All the fields in the **Action details** section are enabled.

9 Make appropriate changes and click **Update action**.

10 To apply this configuration to the server, click **Apply**.

Saving alarm filter files

To save Alarm filter files

1 In the **Alert Filter Configuration** dialog box, click **Save to file**. The **Save alert filters to file** dialog box is displayed

2 By default, the configurations are saved in **alert.filters** file located in the <IEMS Home>/conf directory. Specify a different filename, if required. The relative base directory for saving these files is the <IEMS Home> directory.

3 Click **Save**.

Loading alarm filter files

Previously saved Alarm filters can be loaded to the existing filter list

To load an Alarm filter file

1 In the **Alert Filter Configuration** dialog box, click Load from file. The Load alert filters from file dialog box is displayed

2 Specify the filename

3 Click **Load.**

Note: Any Filter with the same match criteria as that of the existing ones currently listed in the Configured filters list is replaced with the Alarm Filters from the file that you load.

Reordering the configured alarm list

In the Alert Filter Configuration dialog box, click and drag the Alarm Filter you want to reorder in the **Configured filters** list to a new location in the list.

Enabling and disabling alarm filters

The configured Alarm Filter can be enabled or disabled using the enable parameter in the alert.filters file located in the <IEMS Home>/conf directory.

<ALERT_FILTERS>

<FILTER **enable="true"** name=”FilterName”>

<FILTER_ACTION className=”com.adventnet.nms.eventdb.UserFilter”

```
name=”EXAMPLE”
userclass=”com.adventnet.nms.eventdb.UserFilter” />

</FILTER>

</ALERT_FILTERS>
```

If the enable value is set “true” (default value), the corresponding Filter is enabled; and if it is set “false”, it is disabled.*The enabling/disabling of Alarm Filter can be done only by editing the alert.filters file and not through the Alert Filter Configuration tool.*

Deleting alarm filters

To delete an alert filter

1 In the **Alert Filter Configuration** dialog box, select the Alarm Filter to be deleted from the **Configured filter** list

2 Click **Delete** in **Alert filter** section.

3 Click **Yes** to delete the Alarm Filter

To delete an action in an alert filter

4 In the Alert Filter Configuration dialog box, select the Alarm Filter in which the action is to be deleted from the **Configured filters** list.

5 Select the action from Configured filter actions list.

6 Click **Delete** in Alert filter action section.

7 Click **Yes** to delete the action configured for the Alarm Filter.

Example of how to configure the system to send an email on alarm generation

This section describes an example where the operator *Rick* configures the system to send an e-mail to the administrator *John* with the message “An Alert of Category <CATEGORY> and severity <SEVERITY> has been generated from <SOURCE>. It has been picked up by an <OPERATOR>” when a critical (severity 1)alarm is generated for “other” devices.

> ***Note:*** An alarm can be generated with many defined properties, but they are not taken into consideration in this example.

In the Alert filter configuration tool, do the following:

In the Alert filter section of the tool

1 Click the **Add** button.

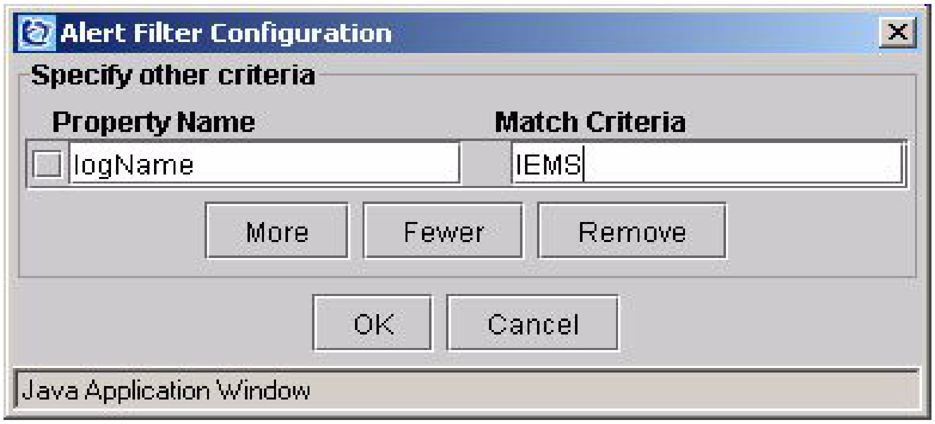
2 Type *Example* in the **Alert filter name** field.

3 Type *1* in the **Severity** field.

4 Type *other* in the **Category** field.

5 Click the **More** button.The **Alert Filter Configuration** dialog is displayed.

6 Type *logName* in the **Property Name** field and *IEMS* in the **Match Criteria** field of the **Alert Filter Configuration** dialog.



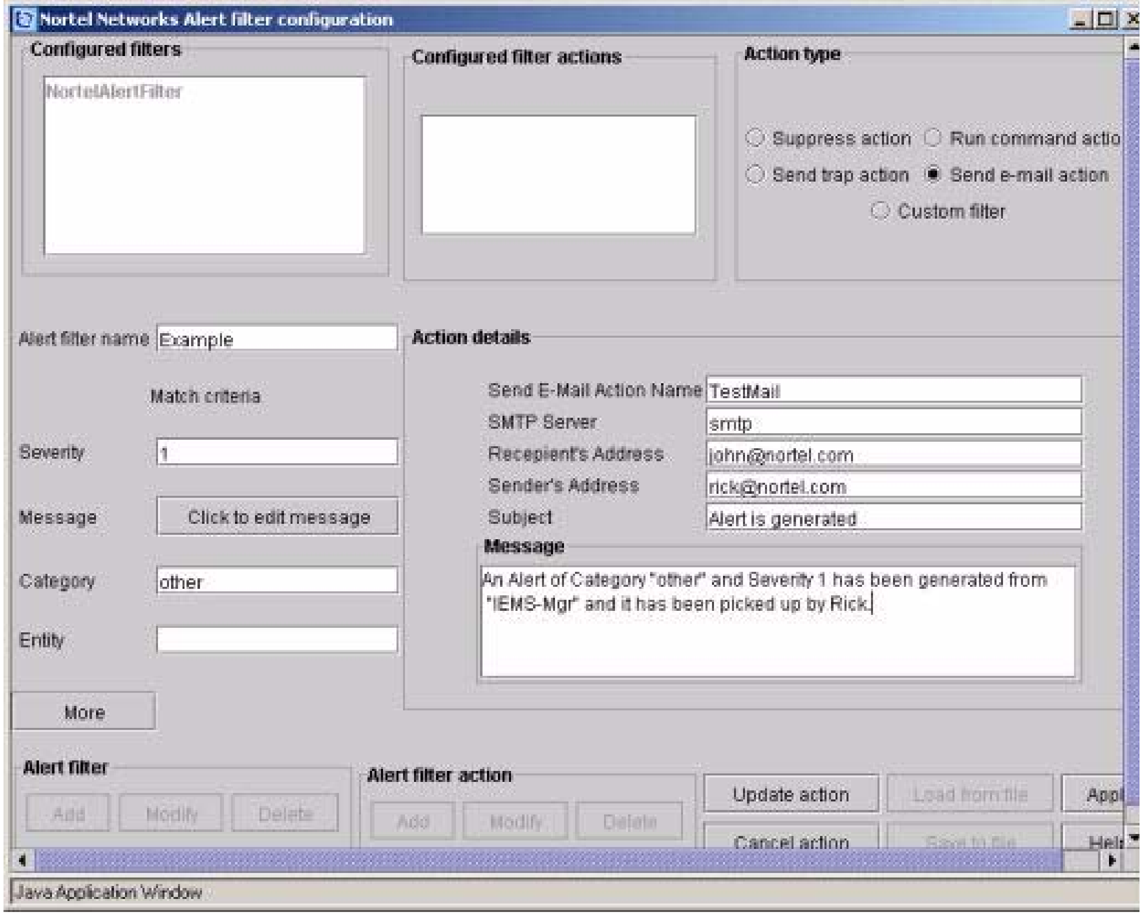
Alert Filter Configuration

Specify other criteria

Property Name	Match Criteria
□ logName	IEMS

7 Click the **OK** button of the **Alert Filter Configuration** dialog.

8 In the **Alert filter action** panel of the tool, click the **Add** button.



NortelAlertFilter

○ Suppress action ○ Run command actio
○ Send trap action ● Send e-mail action
○ Custom filter

Alert filter name	Example
Match criteria	
Severity	1
Message	Click to edit message
Category	other
Entity	

Action details

Send E-Mail Action Name	TestMail
SMTP Server	smtp
Recipient's Address	john@nortel.com
Sender's Address	rick@nortel.com
Subject	Alert is generated

Message

An Alert of Category "other" and Severity 1 has been generated from "IEMS-Mgr" and it has been picked up by Rick.

9 Select the **Send e-mail action** radio button from the **Action type** section.

10 Type *TestMail* in the **Send E-mail Action Name** field of the **Action details** panel.

11 Type the SMTP server name (of the machine for which the alert is configured) in the **SMTP Server** field.

12 Type *john@nortel.com* in the **Recipient's Address** field.

> ***Note 1:*** You can include multiple recipient's e-mail ids by using comma separator.
>
> ***Note 2:*** E-mails addressed to cell phone e-mails ids can be sent from the alert filter GUI. These e-mails can be converted to short text messages and transmitted to the cellphone users by the cellphone service providers must have the provision to convert e-mails to short text messages and dispatch them to the respective users.

13 Type *rick@nortel.com* in the **Sender's Address** field.

14 Type the subject of the mail in the **Subject** field. For example, *Alert is generated*.

15 Type the message *An alert of Category "other" and Severity "1" has been generated from <device name> and it has been picked up by Rick* in the **Message** field.

16 Click the **Update action** button.

17 Click the **Apply** button.

On executing this example, a mail is sent for the alarm of severity *1* and of device category as *other*, to John with the following message.

"An Alert of Category "other" and Severity 1 has been generated from <device name> and it has been picked up by Rick".

Configuring the destination for SNMP traps

Application

Use this procedure to configure the destination for SNMP traps on the Integrated Element Management System (EMS) server and other Succession Server Platform Foundation Software (SSPFS)-based servers that need to forward their SNMP traps to the Integrated Element Management System (EMS) application.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the server on which you are configuring the destination for SNMP traps
- you need the IP address of the server where the Integrated Element Management System (EMS) resides

> ***Note:*** You can obtain the Integrated EMS IP address to use as the destination for SNMP traps, by logging in to the Integrated EMS server and executing the command “getpip.ksh IEMS”.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the SSPFS-based server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the server on which you are configuring the destination for SNMP traps

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5. Access the command line interface by typing

   ```
   # cli
   ```

   and pressing the Enter key.

   Example response

   ```
   Command Line Interface
    1 - View

    2 - Configuration

    3 - Other


    X - exit

   select -
   ```

6. Enter the number next to the “Configuration” option in the menu.

   Example response

   ```
   Configuration
    1 - NTP Configuration
    2 - Apache Proxy Configuration
    3 - DCE Configuration
    4 - OAMP Application Configuration
    5 - CORBA Configuration
    6 - IP Configuration
    7 - DNS Configuration
    8 - Syslog Configuration
    9 - Database Configuration
   10 - NFS Configuration
   11 - Bootp Configuration
   12 - Restricted Shell Configuration
   13 - Security Services Configuration
   14 - Login Session
   15 - Location Configuration
   16 - Cluster Configuration
   17 - Succession Element Configuration
   18 - snmp_poller (SNMP Poller Configuration)

    X - exit


   Select -
   ```

7 Enter the number next to the “Succession Element Configuration” option in the menu.

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

8 Enter the number next to the “RESMON Application Configuration” option in the menu.

Example response

```
RESMON Application Configuration
  1 - settrapdest (Set location for IEMS traps)
  2 - queryFaults (Query all faults on the box)
  3 - enableLocalLogs (Enable Local Logging Of
      Faults)
  4 - disableLocalLogs (Disable Local Logging Of
      Faults)


 X - exit

select -
```

9 Enter the number next to the “settrapdest” option in the menu.

Example response

```
===Executing “settrapdest”

Enter the IEMS Server IP Address (default:
45.123.456.78):
```

10 When prompted, enter the IP address of the server where the Integrated EMS resides, or press the Enter key to accept the default if one is specified.

> ***Note:*** You can obtain the Integrated EMS IP address to use as the destination for SNMP traps, by logging in to the Integrated EMS server and executing the command “getpip.ksh IEMS”.

Example response

```
IEMS IP: 45.123.456.78

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

11 When prompted, confirm the IP address you entered by typing

ok

and pressing the Enter key.

Example response

```
===”settrapdest” completed successfully

RESMON Application Configuration
  1 - settrapdest (Set location for IEMS traps)
  2 - queryFaults (Query all faults on the box)
  3 - enableLocalLogs (Enable Local Logging Of
      Faults)
  4 - disableLocalLogs (Disable Local Logging Of
      Faults)


 X - exit

select -
```

12 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

13 You have completed this procedure.

Configuring the Event Cleanup interval

Integrated EMS can configure the Event Cleanup interval in Integrated EMS Client. The events in the Integrated EMS database are cleaned up in the regular intervals specified.

To configure the Event Cleanup Interval, follow these steps:

At the Integrated EMS workstation

1. Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).
2. Select the **Tools-->Event Cleanup** menu command to launch the dialog.
3. Type the required interval (in days) in the field provided.
4. Click the **OK** button to close the dialog.

Note: The default Event Cleanup Interval is 7 days.

Changing attributes for SNMP fault feeds

Integrated EMS administrator can change the attributes and SNMP v3 attributes for SNMP northbound fault feeds. Integrated EMS stores these attributes in <IEMS Home>/conf/NMSProcessesBE.conf configuration file (for SNMP attributes) and <IEMS Home>/conf/<IEMS Home>/conf/mediationagent/v3entries.xml file (for SNMP v3 attributes), where <IEMS Home> is the home directory of Integrated EMS installation directory. The attributes apply only to the Integrated EMS SNMP northbound interface. The attributes are changed using the SNMP configurator command line tool.

Changing SNMP attributes for SNMP northbound fault feeds

The SNMP attributes for SNMP northbound fault feeds can be changed using SNMP Configurator command line tool. The SNMP Configurator command line tool (snmpConfigurator.sh) is present under <IEMS Home>/bin, where <IEMS Home> is the home directory of Integrated EMS installation directory.

Changing all the SNMP attributes

To change the values of all SNMP attributes for SNMP northbound fault feeds, follow these steps:

At the Integrated EMS workstation

1 Connect to the host in which Integrated EMS server is running using telnet.

2 Type the following command and press the **Enter key to change to the directory bin**.

```
cd bin
```

3 Type the following command and press the Enter key to execute the SNMP Configurator command line tool. Enter “2” and press the **Enter** key to select the “Edit” option.

```
#sh snmpConfigurator.sh
Configure the Agent Settings:
(0) Exit
(1) View
(2) Edit
Enter your Choice:2
```

4 Enter "5" and press the Enter key to edit all the SNMP attributes.

```
Choose the Configuration you wish to change
(0) Exit

(1) Agent Port

(2) Agent Version

(3) Agent Community

(4) Vacm

(5) All

Enter your Choice: 5
```

5 Enter the required agent port and press the Enter key. The Agent Port must be within the range 0-65535.

Example
Enter “8001” and press the Enter key

```
Agent Port(0 - 65535):8001
```

6 Enter the agent version (v1, v2, or v3) and press the Enter key.

Example
Enter “v1” and press the Enter key

```
Snmp Agent Version (v1/v2c/v3):
```

7 Enter the community string and press the Enter key. If you are entering more than one community string, separate them using a semicolon (;).

Example
Enter “public” and press the Enter key

```
Communities separated by “;”:public
```

The following message is displayed to complete the changes.

```
Completed Modifying the Settings

!!!! Agent has to restarted for the changes
made!!!!
```

8 Enter "Y" to restart the agent and press the Enter key.

```
Would you like to restart the Agent for the
changes to take effect (Y/N):Y
```

If the agent does not require restart, enter "N" and press the Enter key.

Changing the agent port attribute

To change the agent port SNMP attribute, follow these steps:

At Integrated EMS workstation

1 Refer to the step 1 to step 3 of Procedure .

The various options of SNMP Configurator command line tool are listed below:

Enter "1" and press the Enter key.

```
Choose the Configuration you wish to change
(0) Exit

(1) Agent Port

(2) Agent Version

(3) Agent Community

(4) Vacm

(5) All

Enter your Choice: 1
```

2 Refer to the step 5 of Procedure .

The following message is displayed.

```
Completed Modifying the Settings

!!!! Agent has to restarted for the changes
made!!!!
```

3 Refer to the step 8 of Procedure .

Changing the agent version attribute

To change the agent version SNMP attribute, follow these steps:

At Integrated EMS workstation

1 Refer to the step 1 to step 3 of Procedure .

The various options of SNMP Configurator command line tool are listed below.

Enter "2" and press the Enter key.

```
Choose the Configuration you wish to change
(0) Exit

(1) Agent Port

(2) Agent Version
```

```
(3) Agent Community

(4) Vacm

(5) All

Enter your Choice: 2
```

2 Refer to the step 6 of Procedure .

The following message is displayed.

```
Completed Modifying the Settings

!!!! Agent has to restarted for the changes
made!!!!
```

3 Refer to the step 8 of Procedure .

Changing the agent community

To change the agent community SNMP attribute, follow these steps:

At Integrated EMS workstation

1 Refer to the step 1 to step 3 of Procedure .

The various options of SNMP Configurator command line tool are listed below.

Enter "2" and press the Enter key.

```
Choose the Configuration you wish to change
(0) Exit

(1) Agent Port

(2) Agent Version

(3) Agent Community

(4) Vacm

(5) All

Enter your Choice: 3
```

2 Refer to the step 7 of Procedure .

The following message is displayed.

```
Completed Modifying the Settings

!!!! Agent has to restarted for the changes
made!!!!
```

3 Refer to the step 8 of Procedure .

Changing SNMP v3 attributes for SNMP northbound fault feeds

The SNMP v3 attributes for SNMP northbound fault feeds, such as user name, context name, authorization password, privacy password, and authorization protocol. This is achieved by modifying the corresponding attributes using the SNMP Configurator command line tool(snmpConfigurator.sh), present under <IEMS Home>/bin where the Integrated EMS Server is running.

To change the SNMP v3 attributes for SNMP northbound fault feeds, follow these steps:

At the Integrated EMS workstation

1 Refer to the step 1 to step 3 of Procedure .

The various options of SNMP Configurator command line tool are listed below.

Enter “2” and press the Enter key.

```
Choose the Configuration you wish to change
(0) Exit

(1) Agent Port

(2) Agent Version

(3) Agent Community

(4) Vacm

(5) All

Enter your Choice: 4
```

Note: The SNMP version of SNMP northbound fault feed must be v3 to change the SNMP v3 vacm attributes. If the version is other than v3, the “Change the Version before configuring Vacm” message is displayed and prompts you to change the SNMP version. Repeat the step 2 to change the agent version.

Using Other Administrative Operations

Integrated EMS administrator can configure the event cleanup, log settings, client retry time, and printer. In addition, the administrator can modify the attributes for the SNMP fault feeds and security notice message displayed during startup of the client. Besides, the Runtime Administration tool (accessed from the “Tools” menu command) facilitates configuring certain administrative tasks through its intuitive GUI.

This section explains these functions in the following sections:

- Viewing audit and security logs
- Configuring the client retry time
- Changing the security notice text
- Configuring the printer
- Using the Runtime Administration tool
  - Configuring log settings

Backup and Restore Procedure in Integrated EMS

As Integrated EMS resides on the SSPFS platform, it executes the backup and restore policy defined for the SSPFS platform. For more details on the backup and restore procedures, refer to the ATM/IP Solution-level Security and Administration, NN10402-600.

Viewing audit and security logs

Integrated EMS administrators can view the audit log details of the administrative operations and the security log details of the security related operations and the authentication details through the client GUI. The log messages are stored in the log files of <IEMS Home>/var/log directory. This section explains details of both the audit and security logs, which can be viewed from the client GUI.

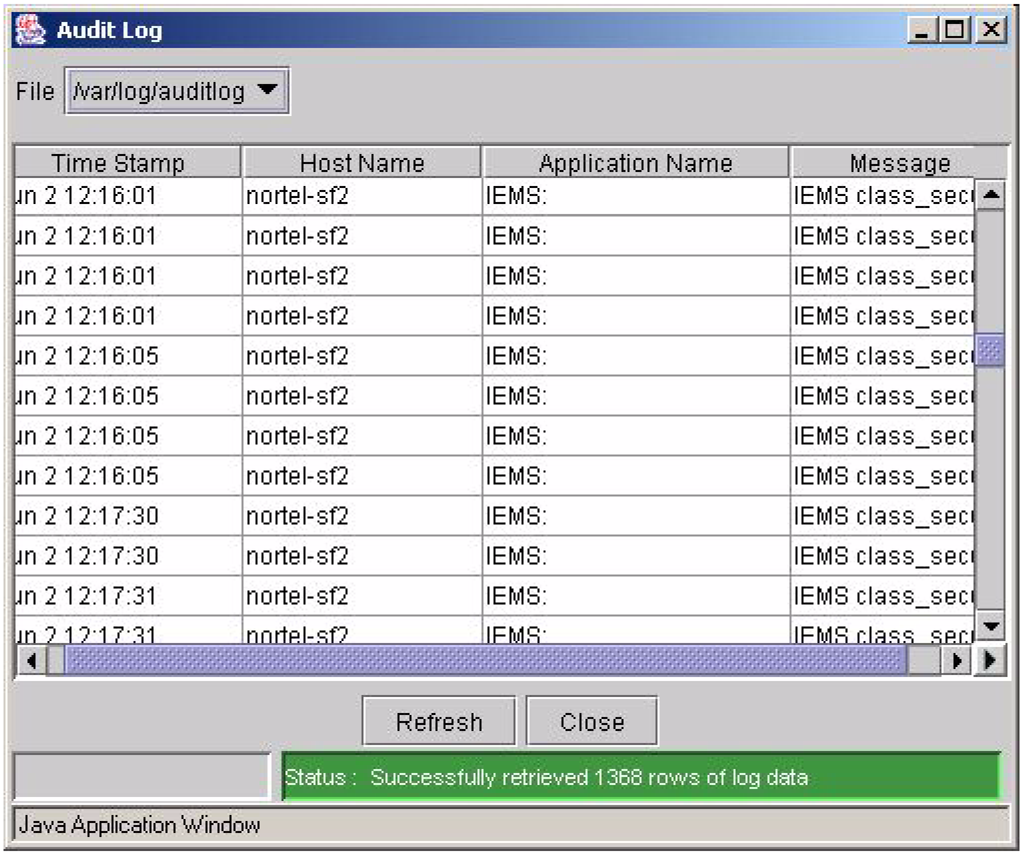
Viewing audit logs

At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Tools-->Audit Logs** menu command to view the audit logs.

3 The **Audit Log** window as shown below is displayed.



File /var/log/auditlog

Time Stamp	Host Name	Application Name	Message
un 2 12:16:01	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:01	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:01	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:01	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:05	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:05	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:05	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:16:05	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:17:30	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:17:30	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:17:31	nortel-sf2	IEMS:	IEMS class_sec
un 2 12:17:31	nortel-sf2	IEMS:	IEMS class_sec

Status : Successfully retrieved 1368 rows of log data

Definition of attributes in Audit Log window

Table column name	Description
Time Stamp	This attribute indicates the time at which the log messages are generated.
Host Name	This indicates the name of the host in which the Integrated EMS is running.
Application Name	This indicates the name of the application (running on SSPFS) for which the logs are generated.
Message	This is the log message, which indicates the state of the executing operation.

Viewing security logs

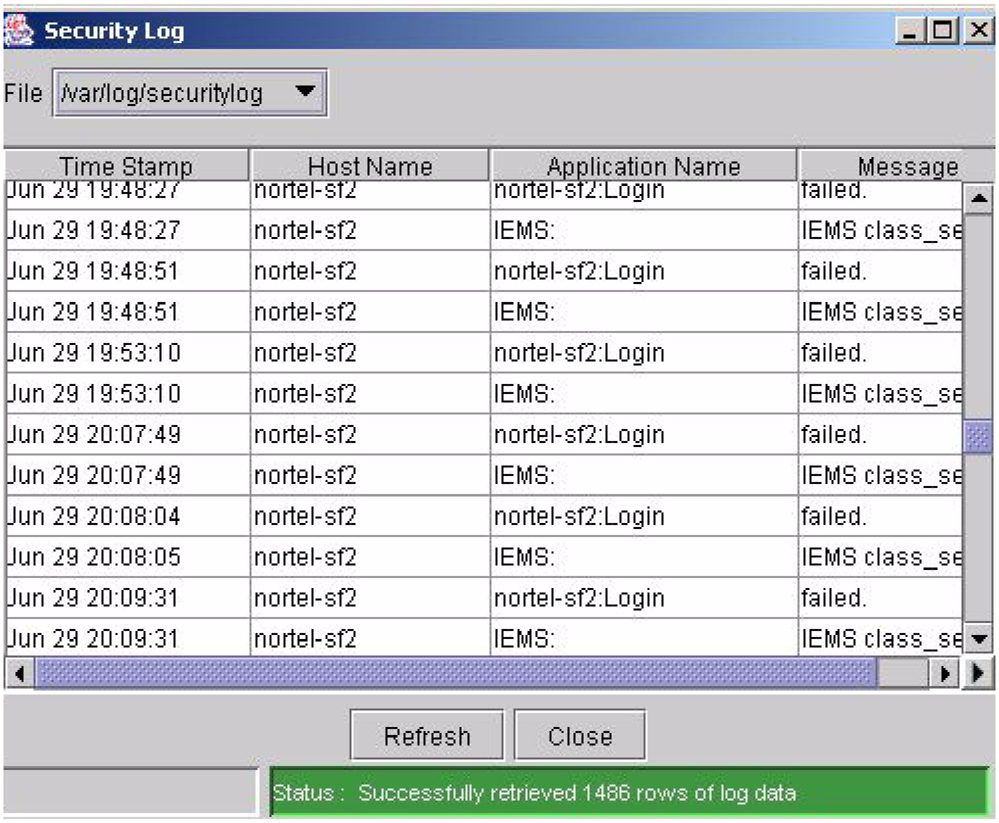
At the Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to the “Launching Integrated EMS Java Web Start Client” of Integrated EMS Basics, NN10329-111).

2 Select the **Tools-->Security Logs** menu command to view the security logs.

3 The **Security Log** window as shown below is displayed.

> ***Note:*** The description of the fields in the **Security Log** window is same as that explained in the table above for the **Audit Log** window.



File /var/log/securitylog

Time Stamp	Host Name	Application Name	Message
Jun 29 19:48:27	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 19:48:27	nortel-sf2	IEMS:	IEMS class_se
Jun 29 19:48:51	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 19:48:51	nortel-sf2	IEMS:	IEMS class_se
Jun 29 19:53:10	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 19:53:10	nortel-sf2	IEMS:	IEMS class_se
Jun 29 20:07:49	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 20:07:49	nortel-sf2	IEMS:	IEMS class_se
Jun 29 20:08:04	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 20:08:05	nortel-sf2	IEMS:	IEMS class_se
Jun 29 20:09:31	nortel-sf2	nortel-sf2:Login	failed.
Jun 29 20:09:31	nortel-sf2	IEMS:	IEMS class_se

Status : Successfully retrieved 1486 rows of log data

Configuring the client retry time

When the Integrated EMS Server stop or shutdown in unforeseen circumstances, the Integrated EMS Java Web Start Client tries to reconnect the Integrated EMS Server for a certain period. This certain period is known as Client Retry Time. The Client Retry Time is modified by changing the value for MAX_RETRY_PERIOD parameter in clientparametes.conf file present under <IEMS Home>/conf directory.

To change the security notice text, follow these steps:

At the Integrated EMS workstation

1 Switch to the <IEMS Home>/conf directory in the system where the Integrated EMS Server is installed.

2 Open the file clientparameters.conf using a standard text editor (for example, “vi” in Sun Solaris).

3 Change the value for the MAX_RETRY_PERIOD parameter.

The default value is 300000 milliseconds.

4 Save the file.

5 Restart the Integrated EMS Server to implement the changes.

Note: After modifying the client retry period in clientparameters.conf file, Integrated EMS Server must be restarted.

Changing the security notice text

After you log in (using the Authentication dialog), the system displays a splash screen, then the Security Notice window. Integrated EMS stores the Security Notice text in the editable file securitywarning.txt (present under <IEMS Home>/conf directory where Integrated EMS Server is installed).

To change the security notice text, follow these steps:

At the Integrated EMS workstation

1. Switch to the <IEMS Home>/conf directory in the system where the Integrated EMS Server is installed.
2. Open the file securitywarning.txt using a standard text editor (for example, “vi” in Sun Solaris).
3. Change the text as required.
4. Save the file.
5. Restart the Integrated EMS Server to implement the changes.

Note: After modifying the text in securitywarning.txt file, the Integrated EMS SErver must be restarted.

Configuring the printer

In the Integrated EMS Client, the current range of Events in the selected Events panel can be printed. The printing is carried out from the system where the Integrated EMS Server is located. To execute this action, the Integrated EMS Server must have a configured network printer.

The PRINT_COMMAND parameter in the file NmsProcessesBE.conf present under <IEMS Home>/conf must be configured to enable the print option. The print file argument must be based on the value specified for the SAVE_DIR parameter.

> ***Note:*** By default, the SAVE_DIR parameter is set as the state directory.

The PRINT_COMMAND entry against the EventMgr process in the file NmsProcessesBE.conf must be in the following format:

PRINT_COMMAND "lpr -S Server -P printername <filename>"

where,

-S Server: Server Name of the host, which provides the lpd service.

-P printername: Name of the print queue, which is maintained by the printer (to put the job in the print queue and process it).

<filename>: Name of the file to be printed. This must refer to the SAVE_DIR directory, so the file name must be in the format <value of AVE_DIR>\\printfile.tmp

Example
SAVE_DIR state PRINT_COMMAND “lpr -S Duplex1 -P test state\\printfile.tmp”

where

“-S Duplex1” is the Server Name, “-P test” is the name of the print queue, and “printfile.tmp” is the name of the file to be printed, which is present in the state directory.

> ***Note 1:*** When you execute the print function from the Integrated EMS Client, Integrated EMS temporarily stores all the Event or Alarm details in a file named printfile.tmp. This file is present under the directory configured for the SAVE_DIR parameter in the EventMgr process. The next time the Events are printed, the new details replace the previous details in the file printfile.tmp. process. When

Print is launched next time, those corresponding to the next request replace the details in the printfile.tmp.

Note 2: The system saves and prints only the current range of Events in the selected Events panel of the Integrated EMS Client.

Note 3: After modifying the NmsProcessesBE.conf file, the Integrated EMS Server must be restarted to implement the new printer configuration.

Using the Runtime Administration tool

The Runtime Administration tool is an easy-to-use tool that helps in administering various modules of Integrated EMS, at runtime. Making configurations at runtime using this tool avoids the hassles of restarting the Integrated EMS server every time a configuration is performed. This tool can be accessed though the menu command “**Tools-->Runtime Administration**".

The description of the toolbar buttons of the Runtime Administration tool are in the following table:

Toolbar Button	Description
💾	This tool button is used to save the configuration changes performed through the Runtime Administration GUI, in the Integrated EMS server.
🚪	This tool button is used to close the Runtime Administration tool.
?	This tool button is used to invoke the help related to the Runtime Administration tool.

This tool can be used for configuring the following tasks:

Refer to the following sections of *Integrated EMS Fault Management,* NN10334-911 for configuring Northbound Fault Feeds:

- Configuring SCC2 Northbound Fault Feeds
- Configuring SNMP Northbound Fault Feeds
- Configuring SYSLOG Customerlog Configuration
- Configuring NTSTD Northbound Fault Feeds

Refer to the following sections for configuring log settings:

- Configuring log settings

Configuring log settings

The Logging Service is useful for various purposes, such as pinpointing bugs, configuration errors, performance blockades, creating audit logs, and keeping track of various actions taking place in the server.

All messages are stored in log files in the text format(.txt). All configurations related to these log files are available in the logging_parameter.conf file located in the <IEMS Home>/conf directory. The logging_parameter.conf file contains the entries of various user-specified.text files, the maximum number of lines to be read from a file, and the number of files to be included.

The logging can be configured by editing logging_parameters.conf file using the Runtime Administration tool of Integrated EMS. Using this tool update the file at runtime so that Integrated EMS Server restart is not required after configuration.

> ***Note:*** Note: The Runtime Administration Tool can be used to configure the Server-related log messages only. To configure Client-related logs, manually configure the logging_paramenters.conf file located in the <IEMS Home>/conf directory.

This section describes the procedure for the following tasks:

- Opening the Logging Configuration GUI
- Adding log files
- Viewing details of log files
- Modifying log file details

Opening the Logging Configuration GUI

To open the log file configuration GUI, follow these steps:

At the Integrated EMS workstation

1 Refer to the “Launching Integrated EMS Java Web Start Client” of the *Integrated EMS Basics*, NN10329-111 to launch the Integrated EMS Client.

2 Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.

3 Select the **Log Settings** node under Miscellaneous tree.

The Logging Configuration GUI is displayed in the right hand side frame.

Adding log files

To add a new log file, follow these steps:

At the Integrated EMS workstation

1 Refer to the “Opening the Logging Configuration GUI“section to open the Logging Configuration GUI.

2 Specify the name of the log file in **Log File Name** field.

Note: File names that are compatible with an OS is only supported. Specify the file name extension as.txt. Avoid using numbers in file names.

3 Type the directory where the log file has to be stored in **Logging Directory** field. By default, the log files are stored in <IEMS Home>/logs directory. If you need to specify a directory within this default location, specify logs/<directory name>.

Example
If newlogdir is specified, a new directory is created in <IEMS Home> and the new log file is stored in this location. If logs/newlogdir is specified, a new directory is created in <IEMS Home>/logs directory.

4 Specify the number of lines to be written in the log file in **Maximum Number of Lines Per File** field.

This is an optional field. When no value is specified, the default value of 10000 lines is set

5 When the log file exceeds the maximum number of lines specified, it is carried forward to another new file that is created with similar name. For example, when newfile.txt reaches 10000 lines, then a new file newfile1.txt is created and the logging continues. The number of files that can be created at such cases can be specified in **Maximum Number of Files** field.

This is an optional field. When no value is specified, the default value of 10 is set.

6 Configure the maximum number of lines to be kept in memory before writing them to a log file by typing the value in **Maximum Lines Cached** field. For example, if the value is set as 50, the first 50 lines is kept or cached in memory. On reaching the 50th line, all the 50 lines are written to the log file. Then, the second round of writing happens after caching 50 more lines and so on.

This parameter avoids the overhead of frequent writings into the log file for each line.

7 Check the **Use Time Stamp?** field if the time stamp is required along with log messages.

8 Click the **Next** button.

9 Type the unique key name in **Key Name** field. This serves as the key with which Integrated EMS differentiates between modules to log module-specific log messages and to identify the type of message, such as, output or error message.

10 Type the module-specific name that is to be prefixed with the log message in the log file in **Display Name** field.

11 Click the **Add** button.

12 Select the log level from the **Log Level** list box. If you choose to record the messages belonging to certain level, the messages with levels lower than and equal to the level chosen is recorded. The description for various log levels are described in the table below.

Log Level	Description
Summary	Important messages
Intermediate Messages	Frequently generated log messages
Verbose	Detailed/Error messages
Debug	Composite of above levels and more information for debugging purposes.

Example
If you choose Intermediate, then all the log messages belonging to the Summary and Intermediate is recorded.

13 To enable the logging in this new log file, check the **Enable Logging?** field. If the log file is created with this field unchecked, then the log file is created in the configured directory, but the logging does not occur.

14 Click the **Finish** button.

15 Click the **Apply** button to effect changes on the server-side logging_parameters.conf file.

The success or failure of writing to server-side file is displayed in the Runtime Administration tool status bar.

Viewing details of log files

To add a new log file, follow these steps:

At the Integrated EMS workstation

1 Refer to the "Opening the Logging Configuration GUI"section to open the Logging Configuration GUI.

2 In the Log File Configuration tool, select the log file from the table.

3 Click the **View Details** button.

The Log Details dialog box is displayed.

Modifying log file details

To add a new log file, follow these steps:

At the Integrated EMS workstation

1 Refer to the "Opening the Logging Configuration GUI"section to open the Logging Configuration GUI.

2 In the Log File Configuration tool, select the log file from the table.

3 Click the **Modify** button.

The Logging Configuration dialog box is displayed.

4 Make the necessary changes in the two screens. For information on each of the fields, refer to the "Adding log files"section.

5 Click the **Finish** button.

Administering Integrated EMS with Web Client

In Integrated EMS Web Client, you can manage users, view server logs and shut down server. This section explains the procedure for these operations. For a detailed explanation, follow the sections below:

- Viewing server logs
- Configuring log settings in Web Client
- Configuring user settings with Web Client
    - Adding users
    - Modifying user profiles
    - Removing users

Viewing server logs

The logs are essential for debugging, recovery of server or viewing error messages. In Integrated EMS Web Client, you can view the logs easily. To view the server logs, connecting to server terminal is not required.

To view the server logs in Web Client, follow these steps:

At Integrated EMS workstation

1 Refer to the “Launching Integrated EMS Web Client” to launch the Integrated EMS Client.

2 Click the **Admin** tab.

3 Click the **Logs** node under Server Admin node in Module tree.

The Server Logs page is displayed.

4 Click the file name listed in the page to view the log content in the corresponding file.

Configuring log settings in Web Client

The Logging Service comes handy for various purposes, such as pinpointing bugs, configuration errors, performance blockades, creating audit logs, and keeping track of various actions taking place in the server.

All messages are stored in log files in the form of Text files (.txt). All configurations related to these log files are available in the logging_parameter.conf file located in the <IEMS Home>/conf directory. The logging_parameter.conf file contains the entries of various user-specified.txt files, the maximum number of lines to be read from a file, and the number of files to be included.

You can configure the logging by editing logging_parameters.conf file using the Runtime Administration tool. Using this tool updates the file at runtime.

Configuring log settings

To configure the log settings in Web Client, follow these steps:

At Integrated EMS workstation

1. Refer to the “Launching Integrated EMS Web Client” to launch the Integrated EMS Client.
2. Click the **Admin** tab.
3. Click the **Logging Level** node in the Admin tree.

   The Logging Configuration page is displayed.
4. Click the file name listed in the page to view the log content in the corresponding file.

The displayed page contains the log FileName along with the configurable options, such as MaxLines, FileCount, MaxLinesCached, and LogLevel.

Configurable Options	Description
MaxLines	Specify the number of lines to be written in the log file.
FileCount	When the log file exceeds the maximum number of lines specified, it is carried forward to another new file that is created with similar name. For example, when newfile.txt reaches 10000 lines, then a new file newfile1.txt is created and the logging continues. Specify the maximum number of log files that can be written by Integrated EMS in this field.
MaxLinesCached	This parameter is used to configure the maximum number of lines to be kept in memory before writing them to a log file. For example, if the value is set as 50, the first 50 lines is kept or cached in memory. On reaching the 50th line, all the 50 lines are written to the log file. Then, the second round of writing happens after caching 50 more lines and so on. This parameter avoids the overhead of frequent writings into the log file for each line.
LogLevel	This parameter is used to categorize the log messages into various levels. The four type log levels are • Summary: Denotes important messages, such as TftpAPI bound in registry, SeverityAPI bound in registry, NmsPolicyAPI bound in registry, and other messages. • Intermediate: Denotes frequently generated log messages, such as Registering Session: AUTH_ID, Registering Session: CONFIG_CLIENT, and other messages. • Verbose: Denotes error messages, such as “Cannot get snmp values from 192.168.4.28: Error: Request Timed Outto192.168.4.28”, and other messages. • Debug: Denotes DEBUG messages useful for debugging purposes. This level records all the messages belonging to the above three levels and in addition, it records the messages which help in tracing bugs. The default log level is 3.

Certain log files, such as nmserr.txt, nmsout.txt contain the logging details of various Integrated EMS modules such as Map, Topology, Provisioning, etc.

To configure the logging levels for these modules, follow these steps.

At the Integrated EMS workstation

1 Refer to the “Launching Integrated EMS Web Client” to launch the Integrated EMS Client.

2 Click the **Admin** tab.

3 Click the **Logging Level** node in the Admin tree.

The Logging Configuration page is displayed.

4 click Configure Log Level for <file_name> (for nmserr.txt and nmsout.txt files). The Configure Log Level for <file_name> page is displayed.

5 Select the modules required. Example: TOPOERR of nmserr.txt file whose log level is to be modified.

6 Choose the Logging Level from the drop-down box for the specific module.

7 Click Submit. Click Reset button, if required, to reset to default values

Configuring user settings with Web Client

You can add users, modify user profile and delete users using Web Client. These operations are done using the User Admin tree in Admin tab of Web Client.

Procedure 1 To navigate to User Admin tree in Web Client, follow these steps:

At Integrated EMS workstation.

1 Refer to the “Launching Integrated EMS Web Client” in *Integrated EMS Basics*, NN10329-111 to launch the Integrated EMS Client.

2 Select the **Admin** tab in the Web Client.

3 Select the **User Admin** node in the Module tree.

Expand the User Admin tree to find the sub-nodes Add User, Modify User Profile, and Delete User.

The Web Client allows the Integrated EMS administrator to configure the following user setting tasks.

- Adding users
- Modifying user profiles
- Removing users

Adding users

Adding a new user is an important activity to provide access to the Integrated EMS Server. Operation and Maintenance personnel can be provided a selective Integrated EMS views with restricted access to different modules, such as Topology, Fault Management, and Inventory.

To add the user to Integrated EMS in Web Client, follow these steps:

At Admin tab of Integrated EMS Web Client

1 Refer to the Procedure to navigate to User Admin node of Web Client in the "Configuring user settings with Web Client"section.

2 Click the **Add New User** node from the Module tree.

OR

Click **Add User** option from the User Admin page displayed on right-side frame.

The Add User page is displayed.

3 Enter the unique user name for the user in the **User Name** field.

4 Enter a password in the Password field and confirm the password in the **Confirm Password** field.

5 Select the group(s) to which the user must be a member. The Available group names field lists all the existing groups.

> ***Note:*** If you need to add the user to a new group, select the **Add this user to a new group** check box and enter the name of the new group in the text field.

6 Select the **Password expires in** check box and enter the number of days the password stays valid.

If the **Password expires in** box is not selected, then the password never expires.

7 Select the **Account expires in** check box and enter the number of days the user account stays valid.

If the **Account expires in** check box is not selected, then the user account never expires.

8 Click the **Add User** button to add the user with the following details.

Note: For Solaris and Linux OS machines, if a user name already exists in the machine registor, then the same user cannot be added through the Security administration GUI.

Modifying user profiles

Integrated EMS administrator can change the password, enrollment of groups, and password and account expiry of existing users. This section describes the procedure to modify these details using Web Client.

To modify the user's profile in Web Client, follow these steps:

At Admin tab of Integrated EMS Web Client

1 Refer to the Procedure to navigate to User Admin node of Web Client in the "Configuring user settings with Web Client"section.

2 Click the **Modify User Profile** node from the Module tree.

OR

Click **Modify User Profile** option from the User Admin page displayed on right-side frame.

The Modify User Profile page is displayed.

3 Enter the user name in the **User Name** field for which the user profile has to be modified.

4 Click the **Submit** button.

The Modify Profile page is launched.

5 Select the **Change Password** box if you want to change the login password.

If you select the Change Password field, enter the current password in the Current Password field. Enter the new password in the New Password field and confirm the new password in Confirm Password field.

6 Select the groups to which the user has to be enrolled in the Enrolled groups field using the **-->** and **<--** button.

7 Select the **Modify Password Expiration** box and provide the password expiry duration in days (if required).

> ***Note:*** If the **Modify Password Expiration** was not configured while creating the user, then 0 is displayed, which means the password never expires. Modify the expiration period, if required, by selecting the check box and entering a new value in the text field.

8 Select the **Modify Account Expiration** box and provide the number of days the user account stays valid (if required).

Note: If the **Modify Account Expiration** was not configured while creating the user, then 0 is displayed, which means the user account never expires. Modify the expiration period, if required, by selecting the check box and entering a new value in the text field.

9 Click the **Submit** button to update the changes.

Removing users

The users who are not required have to be removed from Integrated EMS. This section describes the procedure to remove user. Removing a user shall remove the profile of the user.

To remove the user in Web Client, follow these steps:

At Admin tab of Integrated EMS Web Client

1 Refer to the Procedure to navigate to User Admin node of Web Client in the “Configuring user settings with Web Client“section.

2 Click the **Remove User** node from the Module tree.

OR

Click the **Remove User** option from the User Admin page displayed on right-side frame.

The Remove User page is displayed.

3 Enter the user name that has to be removed in the **User Name** field.

4 Click the **Submit** button.

If the user name exists, “User account successfully removed” message is displayed.