Carrier VoIP

IEMS Administration and Security

NN10336-611

Document status: Standard
Document version: 04.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

IEMS Administration and Security

New in this release

Feature changes

These are the following feature changes in this release.

- IPSec Certificate Manager Support

  This feature integrates the Certificate Manager application with IEMS to provide the following capabilities from the IEMS GUI:

  — Add the Certificate Manager as an application to the IEMS topology

  — View Certificate Manager alarms on IEMS

  — Launch the Certificate Manager GUI client from IEMS using single sign-on

- IEMS Call Server 2000 SIP integration

  This feature integrates the new SSLines platform SIP applications. It integrates the management of the fault and performance interfaces of the SSLines platform applications. This feature also includes rebranding changes to the existing Session Server managed object.

- IEMS supports MDM's security interface changes

  The MDM client is moving from a PAM Radius client to a PAM IS Client. You do not need to configure the Radius secret for (I)SN09 or later versions of MDM.

- IEMS Fault Feed Failover Time Reduction

  This feature aims to minimize the downtime for critical services during failover. The feature aims to decrease the IEMS NB agent startup time and IEMS server startup time. It introduces the following changes:

  — reduced IEMS fault feed failover time for critical resources by keeping a redundant server in warm standby mode

  — reduced IEMS OSS visibility outage time. Since the IEMS application also provides OSS log feeds, reducing fault feed failover time reduces the duration of OSS invisibility during outages.

- — a new STANDBY status is reported by the servquery -status command when a redundant server is in warm standby mode. For details, refer to Viewing the IEMS server status in *IEMS Administration and Security*, NN10336-611.

Introduction

This section contains the following:

- configuring security for the IEMS client, including user settings and custom scopes
- assigning operations to users
- shutting down and starting the IEMS server
- administering operations such as printer configuration and changing the security notice text

Configuring security for the IEMS client

A secure IEMS ensures legitimate use of the network, and maintains 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 IEMS server security information. This security information is stored in the database and in a configuration file, namely securitydbData.xml in the */opt/nortel/iems/current/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 IEMS 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. IEMS hierarchy in managing authorization is User - Group - Authorized Scope or Authorized View - Operations.

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

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

- 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 IEMS sub-application) provides facilities for carrying out the above security operations. Using this tool, IEMS 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 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 IEMS operations

The following two subsections describe how to get started:

- "Starting the Security Administration tool" (page 11)
- "Adding a new user" (page 13)

Starting the Security Administration tool

Application

Use this procedure to start the Security Administration tool.

The Security Administration tool is a sub-application of IEMS. The Security Administration tool can be used for adding new users, adding new groups, associating users to groups, configuring user settings and profiles, changing user password, configuring scopes, and assigning operations to groups.

It is also possible to change the password through the Password Configurator GUI. For more details, refer to "Changing user password with the Password Configurator GUI" (page 41).

The iemsadm user is intended to be used for emergency access to the IEMS client. It is recommended that you use a centralized user account when accessing the IEMS client. In comparison with centralized users, the iemsadm has the following limitations.

- the iemsadm user is not allocated a single sign on (SSO) token. As a result, when performing command line or GUI launches from the IEMS client, SSO is not supported.
- complex password rules are not enforced for the iemsadm user.
- the iemsadm user does not support the password change period minimum and maximum thresholds.
- the iemsadm user does not support group authentication logging.

Prerequisites

You can start this tool only if you are a member of the secadm group.

Action

Step	Action
At the IEMS workstation	
1	Refer to "Refer to Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111, to launch the IEMS Client.
2	Select the **Tools-->Security Administration** menu command. *The Security Administration tool opens.* 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 the Security Administration tree

Icon	Description
👤	User account is enabled.
👤⊗	User account is disabled; the user cannot log in until the account is re-enabled.
🔑✗	User password is expired; user cannot log in until password is changed or existing password is re-authorized.
👤	User account has expired.

—End—

Adding a new user

Application

Use this procedure to add a new user.

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

Action

Step	Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).

2 Do one of the following:

- Select the **File-->New-->Add User** menu command.
- Click the Add User button in the toolbar.
- Select the parent node and then right-click on it to select **Users-->Add User** item in the IEMS tree.

The User Administration wizard opens.

3 Enter the user name in the Enter the user name field. Refer to User name compliance rules for setting up the user name.

4 Enter the password and confirmation password in the respective fields. If the password is not provided, a dialog prompts you to enter the password. Refer to the "Configuring password complexity" (page 15) rules for configuring the password.

The following password restrictions must be followed when setting or changing a user password through any security administration system integrated with the IEMS Security Server, including IEMS itself.

- The user name cannot be longer than eight characters.
- Passwords cannot be the same as a user name.
- The password complexities in "Configuring password complexity" (page 15) also apply.

By default, new users have only login permission. You can provide access to various operations either by making them members of existing groups, or by assigning them directly to required operations.

5 Click the **Next** button.

6 Configure the password expiry time period (in days) in the displayed screen. By default, the password expiry is configured for 30 days in the **The password expires every** field.

If you check the **Password never expires** check box, a value of -1 is displayed in the **The password expires every** field.

7 Click the **Next** button.

The User Administration window opens.

8 Select a group for the created user, from among those listed in the **Assign groups for the user** screen. The operations assigned for the specific group can be viewed only by clicking the arrow displayed for the corresponding group in the right-hand side of the screen.

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

The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in IEMS and groups created at the SPFS/Solaris level.

When adding APS users, the "mgcmtc" and "mgcadm" groups must be selected from the Group name(s) list.

9 Click the **Advanced** button.

The **Additional User Details** screen is displayed.

The explanations of the fields are as follows:

Field Name	Description
User ID	The user unique numerical ID for the machine (with a Unix operating system). The ID is auto generated based on the range given in the NmsProcessessBE.conf file of the /opt/nortel/iems/current/conf directory.
Primary Group	The unique numerical ID of the primary group to which the user belongs. You can select the group from the displayed list to which the added user is to be assigned.
Gecos	The user’s real name.
Min (days)	The minimum number of days required between password changes. This insures that an expired password is not immediately reused. By default the value is 1.
Expiry Date	The date when the password can no longer be used.

Field Name	Description
Login Shell	The user initial shell program which has the following two alternatives: **no-access --** the user is disallowed from logging into the platform to obtain shell access.**restricted --** by default, the user is allowed to log into the platform to obtain shell access. The shell *rash* is linked to a restricted shell, which is provided by the platform (if supported), or it is linked to an unrestricted shell. Access to unrestricted operations is available through a su (switch user) command.
Home Directory	The pathname to the directory in which the user is initially positioned on logging in.

10 Click the **OK** button in the **Additional User Details** screen.

11 Click the **Finish** button to add the new user to the IEMS. If you want to make any changes in previous screens then click the **Back** button.

The system creates a new user with the specified permissions. The Security Administration tool displays the new user under the **Users** node in the left-hand navigation pane.

—End—

User name compliance

The following are the rules for setting up a user name.

- The user name cannot have upper case characters.
- The user name cannot start with a number.
- The user name cannot contain any special characters.
- The user name cannot exceed eight characters.

Configuring password complexity

There are certain password complexity rules, which must be followed when specifying the username and password for a user. The password complexity rules can be configured through the defaultUserAttribute.prop configuration file of IEMS. This file is located under the /opt/nortel/iems/current/conf directory. The configured password complexity rules are as follows.

The JWS client must be re-started whenever any of the attribute values (given in the table below) are changed. This enables the changed value of the attribute to take effect.

Attribute Name	**Description**
PASSWD_MIN_LENGTH	The password must contain a minimum of 6 characters. By default, the configured value is 6.
PASSWD_MAX_LENGTH	The password can have a maximum of 256 characters. By default, the configured value is 256.
LOWERCASE_COUNT	The minimum number of lowercase characters that a password must contain. By default, the configured value is 1.
UPPERCASE_COUNT	The minimum number of uppercase character that a password must contain. By default, the configured value is 1.
SPECIAL_CHAR_COUNT	The minimum number of special character that a password must contain. By default, the configured value is 0.
NUMBER_COUNT	The minimum number of number character that a password must contain. By default, the configured value is 1.
SPECIAL_CHARS	When the password is scanned for special characters each of the following characters is considered a special character: ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ " , < . > / ? ’
USERNAME_MAX_LENGTH	The username must contain a minimum of 8 characters. By default, the configured value is 8.

Configuring a default secret for RADIUS clients

You can use IEMS to configure the Remote Authentication Dial-In User Service (RADIUS) secret for the RADIUS clients through the client GUI. Configuring the RADIUS secret includes setting the default secrets, and adding, modifying, and deleting the secrets through the IEMS client GUI.

Only the users in the secadm group are authorized to add, modify, or delete RADIUS secrets.

The four types of RADIUS clients for which the default RADIUS secret can be configured through the IEMS GUI and the corresponding platforms, element managers, and network elements are listed in the following table. The reference sections for adding the RADIUS secret are also listed in the following table:

RADIUS client device profiles	Supported platforms, element managers, network elements	Reference sections for adding RADIUS secret through the Add Platform/EMS/NE GUI
IEMS profile	• SPFS platform (hosting non-coresident CMT, MG 9000 Manager, but excluding CBM). • CS 2000 Core Manager plus its platform SDM.	• "Adding Server Platform Foundation Software (SPFS)" in *IEMS Configuration*, NN10330-511 • "Adding a Communication Server 2000 Core Manager (CS 2000 Core Manager) in *IEMS Configuration*, NN10330-511
MG9K profile	MG 9000 NE	"Adding a Multi-Service Gateway 9000 Manager (MG 9000 Manager)" in *IEMS Configuration*, NN10330-511
Passport profile	• MSS 15000 NE • Media Gateway 7480/15000/20000 NE	• "Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements" in *MSS 15000, MG 15000 & MDM in VoIP Networks - Securing Network Elements*, NN10180-612 • ’Updating the MSS/MG15000 switch when the IEMS RADIUS shared secret changes’ in *Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager*

RADIUS client device profiles	Supported platforms, element managers, network elements	Reference sections for adding RADIUS secret through the Add Platform/EMS/NE GUI
		Administration and Security PT-AAL1/UA-AA1/UA-IP, NN10180-611
PP8600 profile	ERS 8600 NE	"Adding a ERS 8600 NE" in *IEMS Configuration*, NN10330-511

Configuring a default RADIUS secret

Application

Use this procedure to configure a default RADIUS secret through the IEMS.

Action

Step	Action
In the Security Administration tool of IEMS	
1	Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).
2	Select the **Edit-->Default Secrets** menu command. *The Default Radius Secret window opens.*
3	Enter the default secrets for the RADIUS client profile. If you leave a profile field empty, the current default secrets for that profile will be deleted.
4	Click the **Modify** button.
5	You have completed this procedure.

—End—

Updating the RADIUS secret for devices

Application

Use this procedure to update a RADIUS secret for devices.

Once a RADIUS secret is added either through the Default Radius Secret GUI or through the Add Platform/EMS/NE wizard, for the RADIUS or the PAM (Pluggable Authentication Module)-RADIUS clients, it can be updated using the **Update RADIUS Secret** menu command. This menu command can be accessed by the users of the **secadm** group only.

Action

Step Action

In the IEMS GUI

1 Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111 to launch the IEMS Client.

2 Select the RADIUS secret supporting device (refer to preceding table) and right click on it.

3 Select the **Update Radius secret** menu command to update the configured RADIUS secret.

The Radius Secret Configuration dialog is displayed.

4 Check the **Radius Secret** check box for adding the RADIUS secret for the selected device.

A warning message is displayed indicating that the configuring secret will be stored in the IEMS security server (Radius server).

If the RADIUS secret is already configured and stored in the IEMS security server, then the same is displayed in the corresponding textfield. You can update the displayed secret, if required.

If the default RADIUS secret is configured using the *Default Radius Secret* GUI, the secret is stored in the IEMS server. This secret is displayed in the respective text field of the GUI on clicking the **OK** button of the displayed warning message.

5 Click the **Modify** button.

6 You have completed this procedure.

—End—

Configuring the secret for Multiservice Switch and Media Gateway NEs

Application

Use this procedure to configure a RADIUS secret authentication for Multiservice Switch and Media Gateway NEs.

The RADIUS secrets can be provisioned for the Multiservice Switch and Media Gateway NEs from the IEMS client GUI. The auto discovered Multiservice Switch and

Media Gateway NEs from MDM 7.0 and higher are listed in the GUI and you can select the Multiservice Switch and Media Gateway NEs, which authenticates to the IEMS.

Action

Step Action

In the IEMS GUI

1 Launch the IEMS Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111..

2 Select **Tools-->MSS Radius Authentication** menu command.

The NEs are listed in the displayed dialog.

3 Select the check box against the NEs for which the RADIUS secret authentication is to be provided by the IEMS security server.

The RADIUS device parameters for all the selected NEs are added to the IEMS security server.

The default secret configured through the Default Radius Secret wizard is applied to all the auto discovered Multiservice Switch and Media Gateway NEs.

For the unchecked NEs, the RADIUS device parameters are deleted from the IEMS security server.

4 Click the **Modify** button.

5 You have completed this procedure.

—End—

Configuring user settings

The Security Administration tool allows the IEMS administrator to configure the user settings and groups as required.

Listing all groups and users

Application

Use this procedure to obtain a list of all groups and users in the IEMS.

In IEMS, by default, 31 Carrier VoIP groups are created, which are listed in the left pane of the Security Administration tool. Administrators can create users and assign them to any of these existing groups or to any newly created groups. The created users too are listed in the same tool and can be used for specific user-oriented tasks.

Action

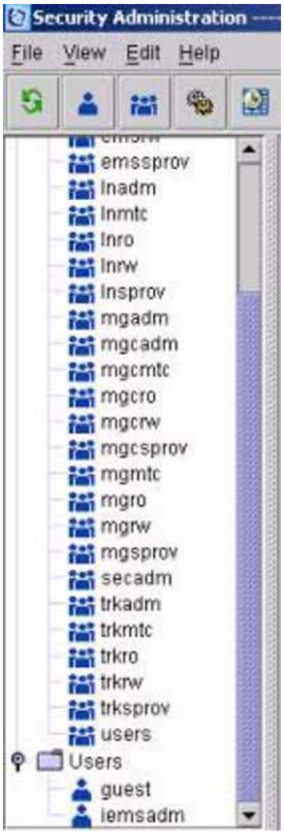
Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (Refer to ""Starting the Security Administration tool" (page 11)").

2 Expand the **Groups** and **Users** nodes in the Security tree as shown in the following figure.

This displays the list of all groups and users, as follows.



emssprov
lnadm
lnmtc
lnro
lnrw
lnsprov
mgadm
mgcadm
mgcmtc
mgcro
mgcrw
mgcsprov
mgmtc
mgro
mgrw
mgsprov
secadm
trkadm
trkmtc
trkro
trkrw
trksprov
users

Users
guest
iemsadm

3 You have completed this procedure.

—End—

User mapping in security administration

The IEMS authorization system allows for the assignment of users to groups, with specific sets of tasks defined for each group. The two legacy IEMS user groups are described below.

admin: The users in this group are permitted to do the following:

- Reconfigure the system.
- Access all functions.
- Set up fundamental configuration.
- Commission (add, delete or rename) the base frames or systems (SAM21 frames, call servers, and large gateways).
- Run service-impacting diagnostics.

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

The IEMS security server also provides 30 application-specific user groups for fine-grained access control. The following table shows the groups with their target network components or applications.

Mapping of user groups for each role in IEMS modules

Groups	Target					
	Line	Trunk	MG (Gateways)	MGC (Call Servers and central components)	EMS/EML	Security
admin	lnadm	trkadm	mgadm	mgcadm	emsadm	secadm
users	lnro	trkro	mgro	mgcro	emsro	secro

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

User mapping with default users

Default user name	Member of group
iemsadm	admin, users

Mapping of IEMS devices to authorization domains

The following table lists the authorization domain that devices in IEMS use. For a description of user groups, see "Setting up local user accounts on an SPFS-Based Server" (page 158)

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 follows:

- "MGC and MG user groups" (page 25)
- "TRK user groups" (page 29)
- "EMS user groups" (page 30)
- "LN user groups" (page 33)
- "SEC user groups" (page 34)

For mapping of CEM user groups to IEMS user group mappings, see "Security group mapping between IEMS and CEM" (page 35).

MGC and MG user groups

	User group									
Command	**mgcadm**	**mgcsprov**	**mgcrw**	**mgcmtc**	**mgcro**	**mgadm**	**mgsprov**	**mgrw**	**mgmtc**	**mgro**
CS 2000 Core										
Launch MAPCI Session	x	x	x	x	x					
GWC (GWC network element)										
GWC Unit Manager	x	x	x	x	x					
Launch Command Line	x									
Launch TMM (see Note 1)	x	x	x	x	x					
Launch LMM (see Note 2)	x	x	x	x	x					
Launch CS 2000 tools (see Note 3)	x	x	x	x	x					
MG 9000 network element										
Update Radius Secret (see Note 4)						x	x	x	x	x

	User group									
Command	**mgcadm**	**mgcsprov**	**mgcrw**	**mgcmtc**	**mgcro**	**mgadm**	**mgsprov**	**mgrw**	**mgmtc**	**mgro**
SAM21										
Launch SCU subnet	x	x	x	x	x					
Launch SCU manager	x	x	x	x	x					
GWC-CARD / CICMEM-CARD/ CICM-CARD / 3PC-CARD /HLR-CARD / MC-CARD /USP-CARD / KDC-CARD /SAM21-UNIT										
Launch SAM21 Card View	x	x	x	x	x					
UAS network element										
Command Line	x	x	x	x	x					
NE-USP / USP										
Launch USP Manager	x	x	x	x	x					
Command Line	x	x	x	x	x					
ERS 8600										
ERS 8600 Device Manager (Launch)	x	x	x	x	x					
ERS 8600 Device Manager (Configure)	x	x	x	x	x					
Command Line	x	x	x	x	x					
Update Radius Secret (see Note 4)	x	x	x	x	x					
Media Server 2000										
Configure MS2000 Automated INI Backup						x	x	x	x	x
Config and Maintenance Tool						x	x	x	x	x
MG 3200										
Configure MG 3200 Automated INI Backup						x	x	x	x	x
Launch Configuration GUI						x	x	x	x	x
IPSec and IKE Config Tool						x	x	x	x	x
STORM										
Launch Command Line	x	x	x	x	x					
Launch STORM Manager	x	x	x	x	x					
SSTrunks NE and Units										
Launch Session Server	x	x	x	x	x					

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmtc	mgcro	mgadm	mgsprov	mgrw	mgmtc	mgro
Command Line	x	x	x	x	x					
Media Application Server										
MAS Manager (P) (Configure)						x	x	x	x	x
MAS Manager (P) (Launch)						x	x	x	x	x
CALL-AGENT-CORE										
Launch MAPCI Session	x	x	x	x	x					
CALL-AGENT-PLAT										
Call Agent Platform Command Line	x	x	x	x	x					
NE-CICM / CICM-Node										
Launch CICM Manager	x	x	x	x	x					
VSP										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Mgr GUI	x	x	x	x	x	x	x	x	x	x
Media Gateway 7480/15000										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Legacy MDM tools	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x
Update Radius secret (see Note 4)	x	x	x	x	x	x	x	x	x	x
Media Gateway 20000										
Client-Server IP provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Legacy MDM tools	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x
MSS - Unknown										
Client-Server IP Provisioning	x	x	x	x	x	x	x	x	x	x
MDM Manager GUI	x	x	x	x	x	x	x	x	x	x
Command Line	x	x	x	x	x	x	x	x	x	x

Command	User group									
	mgcadm	mgcsprov	mgcrw	mgcmtc	mgcro	mgadm	mgsprov	mgrw	mgmtc	mgro
APPLN-APS										
APS Manager (CMT)	x	x	x	x	x					
APS Audio Configuration Tool	x	x	x	x	x					
MTX / MSC / HLR / TRI										
Launch CEM (see Note 5)					x					
IMS/CSE / Media Portal										
Launch MCP System Management Console						x	x	x	x	x
Command Line						x	x	x	x	x
Launch MCS Client (P) (Configure)						x	x	x	x	x
Launch MCS Client (P) (Launch)						x	x	x	x	x
APPLN-OSSGate										
APPLN-OSSGate						x	x	x	x	x
Launch OSSGate						x	x	x	x	x
Launch BPT Servlet						x	x	x	x	x
Launch BPT Command Line						x	x	x	x	x
MCS Manager for MCS/CSE and Media Portal										
Launch MCS Client (P) (Configure)	x	x	x	x	x					
Launch MCS Client (P) (Launch)	x	x	x	x	x					
Launch MCP System Management Console	x	x	x	x	x					
Launch Command Line	x									
MCS Manager for SSLines (see Note 6)										
MCP System Manager Console	x	x	x	x	x					
Configure Session Mgr Platform Command Line (Launch)	x	x	x	x	x					
Session and System Manager Command Line (Launch)	x									
Configure Provisioning Clients	x	x	x	x	x					
MCP Provisioning Client (Launch)	x	x	x	x	x					

	User group									
Command	**mgcadm**	**mgcsprov**	**mgcrw**	**mgcmtc**	**mgcro**	**mgadm**	**mgsprov**	**mgrw**	**mgmtc**	**mgro**
MCS SM Unit / FPM-UNIT										
MCP System Manager Console	x	x	x	x	x					
Command Line	x	x	x	x	x					
EMS-FPM-Mgr										
Launch MCP System Management Console	x	x	x	x	x					
Command Line	x	x	x	x	x					

Note 1: To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group.

Note 2: To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group.

Note 3: To launch CS 2000 tools on a GWC network, the user must be associated with an MGC user group and an EMS user group.

Note 4: To update Radius secret also requires SECADM* privileges.

Note 5: To launch CEM requires MGCRO. Only MGCRO can launch CEM. MGC* cannot launch CEM.

Note 6: Members of ems* and mgc* can launch the MCS Manager in read-only mode. Members of emsadm and emsrw only have configuration or read-write privileges.

TRK user groups

	User group				
Command	**trka**	**trks**	**trkr**	**trkm**	**trkr**

	dm	prov	w	tc	o
GWC (GWC network element)					
Launch TMM (see Note)	x	x	x	x	x
APPLN-TMM					
Trunk Maintenance Manager	x	x	x	x	x
APPLN-OSSGate					
Launch OSSGate	x	x	x	x	x
Launch BPT Servlet	x	x	x	x	x
Note: To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group.					

EMS user groups

	User group				
Command	**emsadm**	**emssprov**	**emsrw**	**emsmtc**	**emsro**
EMS-APS-Mgr (APS Manager)					
APS Manager	x	x	x	x	x
CS 2000 Manager (EMS-CS2K-Mgr)					
Launch Core Manager Maintenance	x	x	x	x	x
Launch MAPCI session	x	x	x	x	x
Update Radius Secret (see Note 1)	x	x	x	x	x
EMS-GWC-Mgr (GWC Manager)					
GWC Manager (CMT)	x	x	x	x	x
GWC Manager Network View	x	x	x	x	x
MG 3200 Manager					
IPSec and IKE Configuration tool	x	x	x	x	x
MG 9000 Manager					
MG 9000 Manager	x	x	x	x	x

Command	User group				
	emsadm	emssprov	emsrw	emsmtc	emsro
IPSec Tool	x	x	x	x	x
EMS-SAM21-Mgr					
SAM21 Manager GUI	x	x	x	x	x
EMS-UAS-Mgr (UAS Manager)					
UAS Manager (CMT)	x	x	x	x	x
CICM Manager (EMS-CICM-Mgr/CICM-Mgr-Node)					
Launch CICM Manager	x	x	x	x	x
Launch Command Line	x	x	x	x	x
MCS Manager for MCS/CSE and Media Portal					
Launch MCS Client (P) (Configure)	x	x	x	x	x
Launch MCS Client (P) (Launch)	x	x	x	x	x
Launch MCP System Management Console					
MCS Manager for SSLines (see Note 2)					
MCP System Manager Console	x	x	x	x	x
Configure Session Mgr Platform Command Line (Launch)	x	x	x	x	x
Session and System Manager Command Line (Launch)	x	x	x	x	x
Configure Provisioning Clients	x	x	x	x	x
MCP Provisioning Client (Launch)	x	x	x	x	x
MCS SM Unit / FPM-UNIT					
MCP System Manager Console	x	x	x	x	x
Command Line	x	x	x	x	x
EMS-FPM-Mgr					
Launch MCP System Management Console	x	x	x	x	x
Command Line	x	x	x	x	x
MDM-Mgr-UNIT					
Update Radius secret (see Note 1)	x	x	x	x	x
EMS-MDM-Mgr					
Client-Server IP provisioning	x	x	x	x	x

Command	User group				
	emsadm	emssprov	emsrw	emsmtc	emsro
MDM Manager GUI	x	x	x	x	x
Legacy MDM Tools	x	x	x	x	x
Change MDM Centralized Account	x	x	x	x	x
Command Line	x	x	x	x	x
Partition NEs	x	x	x	x	x
MDM Operator Client GUI	x	x	x	x	x
Update Radius secret (see Note 1)	x	x	x	x	x
PLAT-SPFS					
Command Line	x	x	x	x	x
Servman Applications Status	x	x	x	x	x
Swact Cluster	x		x		
Restart SPFS	x		x		
Update Radius secret (see Note 1)	x	x	x	x	x
SPFS-UNIT					
Command Line	x	x	x	x	x
Servman Applications Status	x	x	x	x	x
Swact Cluster	x	x	x	x	x
Restart SPFS	x	x	x	x	x
PLAT-SDM					
Command Line	x	x	x	x	x
Update Radius secret (see Note 1)	x	x	x	x	x
PLAT-MDM					
Command Line	x	x	x	x	x
Update Radius secret (see Note 1)	x	x	x	x	x
APPLN-QOS					
Launch Command Line	x	x	x	x	x
APPLN-NPM					

	User group				
Command	**emsadm**	**emssprov**	**emsrw**	**emsmtc**	**emsro**
Command Line	x	x	x	x	x
Note 1: To update Radius secret, the user also requires SECADM* privileges. **Note 2:** Members of ems* and mgc* can launch the MCS Manager in read-only mode. Members of emsadm and emsrw only have configuration or read-write privileges.					

LN user groups

	User group				
Command	**lnadm**	**lnsprov**	**lnrw**	**lnmtc**	**lnro**
GWC (GWC NE)					
Launch LMM (see Note)	x	x	x	x	x
APPLN-LMM					
Line Maintenance Manager	x	x	x	x	x
APPLN-OSSGate					
Launch OSSGate	x	x	x	x	x
Launch BPT Servlet	x	x	x	x	x
Launch BPT Command Line	x	x	x	x	x
Note: To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group.					

SEC user groups

Command	User group				
	secadm	secsprov	secrw	secmtc	secro
CS2k Manager (EMS-CS2K-Mgr)					
Update Radius Secret (also requires EMS* privileges)	x				
MG 9000 NE					
Update Radius Secret (also requires MG* privileges)	x				
ERS 8600					
Update Radius Secret (also requires MGC* privileges)	x				
VSP					
Update Radius Secret (also requires MGC* or MG* privileges)	x				
MDM-Mgr-UNIT					
Update Radius Secret (also requires EMS* privileges)	x				
EMS-MDM-Mgr					
Update Radius Secret (also requires EMS* privileges)	x				
Media Gateway 7480/15000					
Update Radius Secret (also requires MGC* or MG* privileges)	x				
PLAT-SPFS					
Update Radius Secret (also requires EMS* privileges)	x				
PLAT-MDM					
Update Radius Secret (also requires EMS* privileges)	x				

Security group mapping between IEMS and CEM

The following table lists the CEM user group or client function to the user group mapping. For more information about CEM user groups, see *CEM Administration and Security*, 411-8111-942.

CEM client function to user group mapping

User groups / client function	User group					
	mgcsprov	mgcmtc	mgcro	emsadm	emsrw	emsmtc
PMUser (can set thresholds on EMS)					X	
FMUser (can clear/acknowledge alarms on EMS)						X
CMUser (can provision network elements)	X					
CTUser (can perform call trace on a network element)		X				
CEMAdminUser (can change user groups on EMS)				X		
Observer (Read only)			X			

Associating a user with groups

Application

Use this procedure to associated users with groups.

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

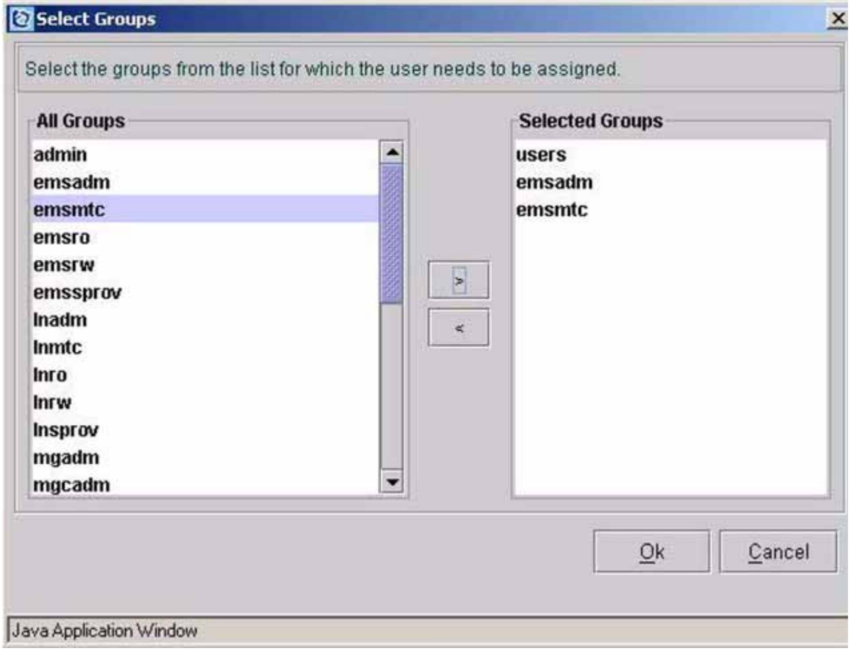
Due to Sun Solaris restrictions, NsSwitch will return only a maximum of 4K characters when getting group information for a user or a group. Therefore, the combined user names in a given user group (including comma characters separating user names) cannot exceed 4075. In a worst case scenario (that is, with 8-character user names), the number of user names that can be mapped to a group is 452.

This limitation is seen when using the internal Central Security System or an external, customer provided Central Security System. Even if the external system can assign more than 452 users per group, the additional userids are not supported.

When the 4K limitation is exceeded, then NsSwitch will return an error code of NSS_NOT_FOUND for associated queries.

Action

Step	Action
In the Security Administration tool of IEMS	
1	Launch the Security Administration tool (refer to "Starting the Security Administration tool" (page 11)).
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
admin
emsadm
emsmtc
emsro
emsrw
emssprov
lnadm
lnmtc
lnro
lnrw
lnsprov
mgadm
mgcadm

Selected Groups
users
emsadm
emsmtc

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.

6 To remove the user from the already associated group, select the group from the Selected Groups list and click the < (Remove) button.

7 Click the **OK** button to update the User and Group details in IEMS Server.

8 You have completed this procedure.

—End—

Setting a user profile

Application

Use this procedure to set the user profile.

The users of the *secadm* group can change the user profile details such as user status, password, account termination, and password expiry.

Action

Step Action

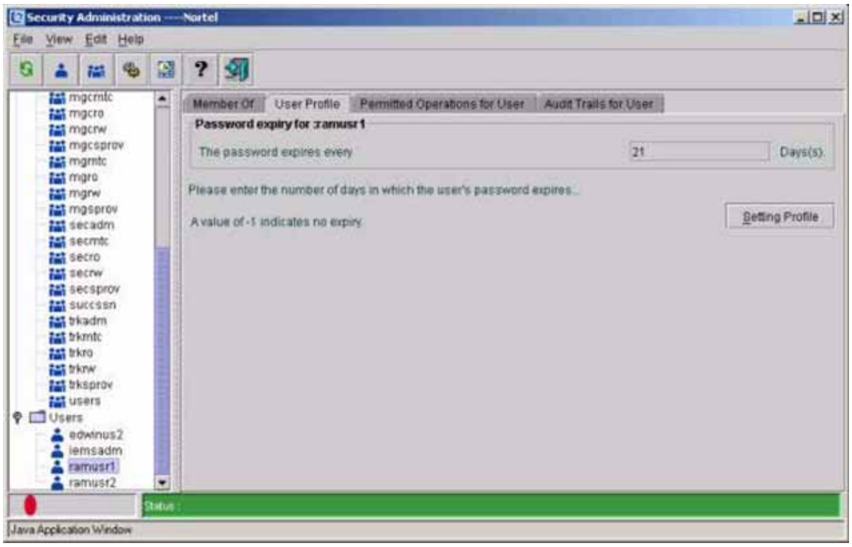
In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to "Starting the Security Administration tool" (page 11)).

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's password expiry status as shown in the following figure:



Password expiry for :ramusr1

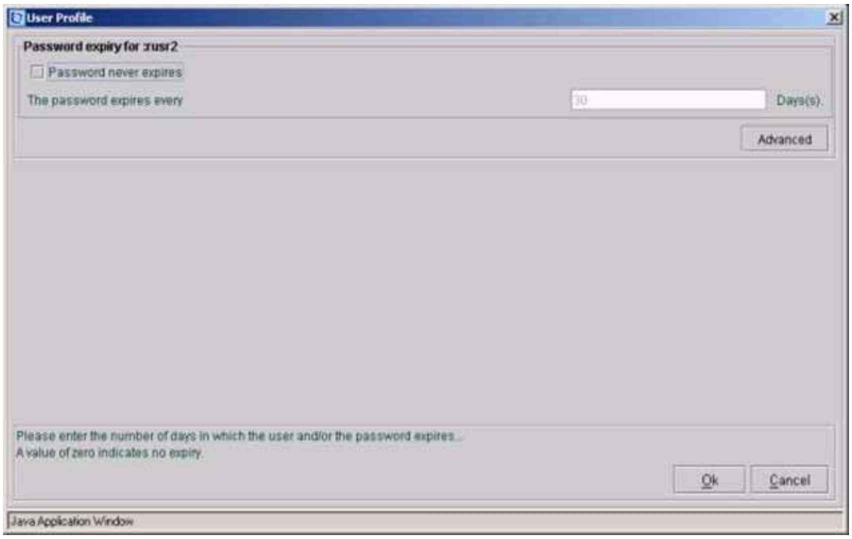
The password expires every 21 Days(s)

Please enter the number of days in which the user's password expires..

A value of -1 indicates no expiry

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

Password expiry for :usr2

□ Password never expires

The password expires every 30 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 password expiry time period by unchecking the **Password never expires** check box and typing the required number of days for the The password expires every field.

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

6 Click the **Advanced** button to invoke the Additional User Details window and modify the same. For more details on the user details properties, refer to the description of the fields for the Additional User Details window in "Adding a new user" (page 13).

7 Click the **OK** button to update the user profile details in the IEMS server.

8 You have completed this procedure.

—End—

Changing user passwords

The users of the secadm group can change the user password for security reasons. User passwords can be changed in the Security Administration GUI or with the Password Configurator GUI. This subsection provides the procedures to change user passwords in these GUIs.

The password restrictions described below must be followed when setting or changing user password through any security administration system integrated with the IEMS Security Server, including the IEMS itself.

- The user name cannot be longer than eight characters.
- Passwords cannot be the same as a user name.
- The password complexities mentioned in "Configuring password complexity" (page 15) also apply.

Refer to the "Configuring password complexity" (page 15) section for more details on the password complexity rules.

Changing a user password in the Security Administration GUI

Application

Use this procedure to change user passwords in the Security Administration GUI.

Action

Step **Action**

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).

2 Select the required user from the Security tree.

3 Do one of the following: to launch the Change Password dialog.

- Select **Change Password** from the Edit menu.
- Right-click on the user in the Security tree and select the **Change Password** menu item.

The Change Password dialog box opens.

4 Type the new password in the New Password field.

5 Confirm the new password in the Confirm Password field.

6 Click the **OK** button to update the password in the IEMS server.

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

7 You have completed this procedure.

—End—

Changing a user password with the Password Configurator GUI

Application

Use this procedure to change the password with the Password configurator GUI for the user currently logged in.

The user can change the user password using the Password Configurator dialog in the IEMS Client user interface.

Action

Step Action

At the IEMS workstation

1 Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111 to launch the IEMS client.

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

3 Type the new password in the New Password field.

4 Confirm the new password in the Confirm Password field.

5 Click the **OK** button to update the password in the IEMS server.

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

6 You have completed this procedure.

—End—

Assigning operations to users

Application

Use this procedure to assign operations to users.

The IEMS administrator can assign various operations to a user. These can be additional operations, which are not authorized via the user's group.

Action

Step Action

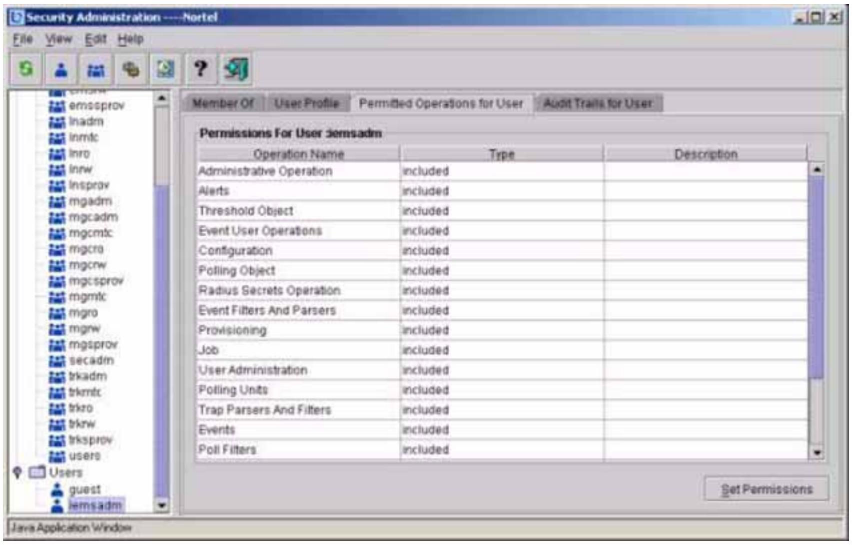
In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to "Starting the Security Administration tool" (page 11)).

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.

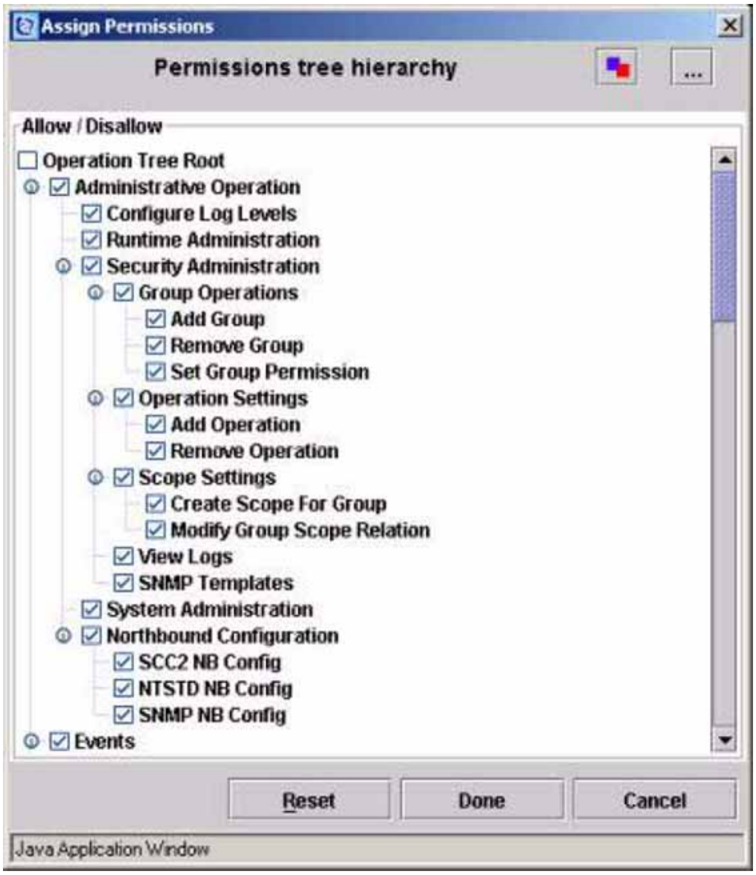


Permissions For User iemsadm

Operation Name	Type	Description
Administrative Operation	included	
Alerts	included	
Threshold Object	included	
Event User Operations	included	
Configuration	included	
Polling Object	included	
Radius Secrets Operation	included	
Event Filters And Parsers	included	
Provisioning	included	
Job	included	
User Administration	included	
Polling Units	included	
Trap Parsers And Filters	included	
Events	included	
Poll Filters	included	

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

This opens the Assign Permissions dialog.



- □ Operation Tree Root
  - ☑ Administrative Operation
    - ☑ Configure Log Levels
    - ☑ Runtime Administration
    - ☑ Security Administration
      - ☑ Group Operations
        - ☑ Add Group
        - ☑ Remove Group
        - ☑ Set Group Permission
      - ☑ Operation Settings
        - ☑ Add Operation
        - ☑ Remove Operation
      - ☑ Scope Settings
        - ☑ Create Scope For Group
        - ☑ Modify Group Scope Relation
      - ☑ View Logs
      - ☑ SNMP Templates
    - ☑ System Administration
    - ☑ Northbound Configuration
      - ☑ SCC2 NB Config
      - ☑ NTSTD NB Config
      - ☑ SNMP NB Config
  - ☑ Events

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).

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 IEMS Server.

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 step 4 to step 6 of this procedure.

7 You have completed this procedure.

—End—

Viewing, saving, and clearing audit trails

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

It is recommended that you use a centralized security user account instead of the iemsadm emergency access user account to log into the IEMS GUI. If you use the iemsadm user account, some user actions such as launching the command line are not recorded in audit trails.

This subsection provides the following procedures:

- viewing audit trails
- saving audit trails
- clearing audit trails

Viewing audit trails

Application

Use this procedure to view the audit trails of all the users in the IEMS.

Action

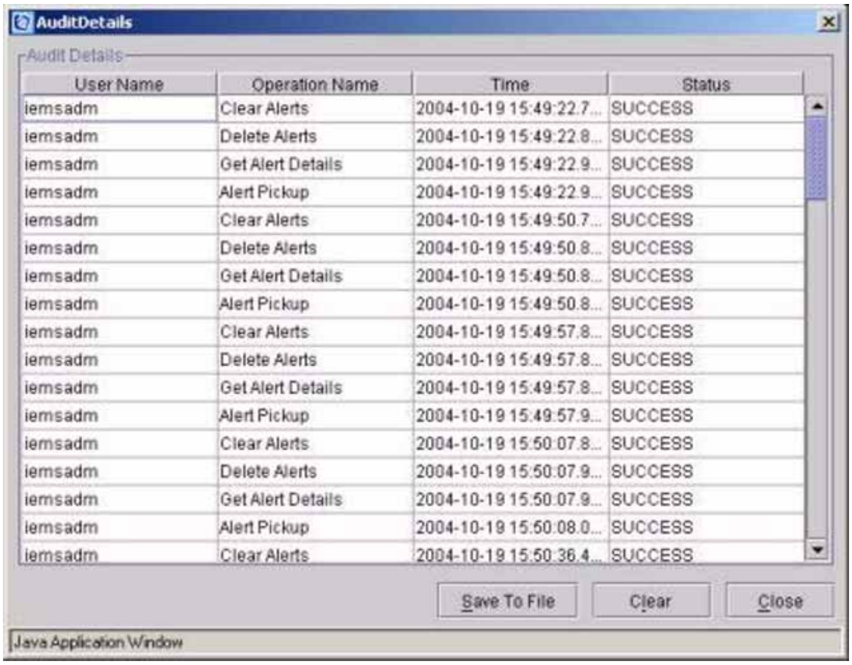
Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to "Starting the Security Administration tool" (page 11)).

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

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



User Name	Operation Name	Time	Status
iemsadm	Clear Alerts	2004-10-19 15:49:22.7...	SUCCESS
iemsadm	Delete Alerts	2004-10-19 15:49:22.8...	SUCCESS
iemsadm	Get Alert Details	2004-10-19 15:49:22.9...	SUCCESS
iemsadm	Alert Pickup	2004-10-19 15:49:22.9...	SUCCESS
iemsadm	Clear Alerts	2004-10-19 15:49:50.7...	SUCCESS
iemsadm	Delete Alerts	2004-10-19 15:49:50.8...	SUCCESS
iemsadm	Get Alert Details	2004-10-19 15:49:50.8...	SUCCESS
iemsadm	Alert Pickup	2004-10-19 15:49:50.8...	SUCCESS
iemsadm	Clear Alerts	2004-10-19 15:49:57.8...	SUCCESS
iemsadm	Delete Alerts	2004-10-19 15:49:57.8...	SUCCESS
iemsadm	Get Alert Details	2004-10-19 15:49:57.8...	SUCCESS
iemsadm	Alert Pickup	2004-10-19 15:49:57.9...	SUCCESS
iemsadm	Clear Alerts	2004-10-19 15:50:07.8...	SUCCESS
iemsadm	Delete Alerts	2004-10-19 15:50:07.9...	SUCCESS
iemsadm	Get Alert Details	2004-10-19 15:50:07.9...	SUCCESS
iemsadm	Alert Pickup	2004-10-19 15:50:08.0...	SUCCESS
iemsadm	Clear Alerts	2004-10-19 15:50:36.4...	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.

4 You have completed this procedure.

—End—

Saving audit trails

Application

Use this procedure to save the audit trails of all users in the IEMS.

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

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to "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.

The security audit trails file is saved in a log file under the /opt/nortel/iems/current/logs/auditlogs folder of the IEMS Server.The file name is as follows: iems_sec_audit.<uid>.<MM_dd_yyyy_HH:MM:ss>.log.

Example
iems_sec_audit.iemsadm.May_20_2005_10:20:34.log

To conserve the disk space on the IEMS Server, the log file is compressed as an archive (.gz) file.The archive file name is as follows: iems_sec_audit.<uid>.<MM_dd_yyyy_HH:MM:ss>.log.gz

Example
iems_sec_audit.iemsadm.May_20_2005_10:20:34.log.gz

Once the audit trials are saved in the log file and archived, a dialog opens with the "/var/logs/iems/auditlogs/iems_sec_audit.iemsadm.May_20_2005_10:20:34.log.gz has been saved" message.

The file is saved under the /opt/nortel/iems/current/logs/auditlogs directory only, but the dialog indicates that it is saved under /var/logs/iems/auditlogs, since /opt/nortel/iems/current/logs is a soft link of the /var/log/iems folder.

4 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 /opt/nortel/iems/current directory.

5 You have completed this procedure.

—End—

Clearing Audit Trails

Application

Use this procedure to clear the audit trails of all users in the IEMS.

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

Action

Step	Action
In the Security Administration tool of IEMS	
1	Launch the Security Administration tool (refer to "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 IEMS Server.
4	Click the **Close** button to close the window.
5	You have completed this procedure.

—End—

Deleting user accounts

IEMS administrator must update the user accounts regularly and delete the accounts of users who are not authorized to access the IEMS. To delete a user account you must:

1. Disable the user account in the Security Administration GUI and Token Administration tool.
2. Delete the user account on the SPFS Security client.
3. Delete the user account in the Security Administration tool.

Disabling the user account in the Security Administration GUI and Token Administration tool

Application

Use this procedure to disable a centrally-managed user in the IEMS Server shell.

Action

Step	Action
In the IEMS workstation	
1	Launch the Security Administration tool in IEMS Client. Refer to "Starting the Security Administration tool" (page 11).
2	Select the required user from the Security tree in the navigation pane on the left-hand side.
3	Select the **User Profile** tab.
4	Click the **Setting Profile** button.
5	Under **Status for the user**, disable the **Select the status for this user** field.
6	Select the disable option from the list box. Select the status for this user field.
7	Click the **OK** button. If any user is disabled or deleted through the IEMS Security GUI, the existing Java WebStart client session and HTML client session are terminated and all future login attempts for that user are blocked.
8	Launch the Security Token Administration GUI. Refer to "Launching the IEMS Security Token Administration GUI" (page 192).

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

10 You have completed this procedure.

—End—

Deleting the user account on an SPFS Security Client

Application

Use this procedure to delete the centralized user account on an SPFS Security.

Action

Step Action

At the SPFS Security client

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

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

3 Delete the user home directory using the following command.

```
rm -r /export/home/<user_name>
```

where <user name> is the user name of the user.

4 You have completed this procedure.

—End—

Deleting the user account in Security Administration tool

Application

Use this procedure to delete a centrally-managed user in the IEMS.

To delete locally-managed users, refer to "Deleting local user accounts from an SPFS-based server" (page 180).

Action

Step Action

At the IEMS workstation

1 Launch the Security Administration tool in the IEMS client. Refer to "Starting the Security Administration tool" (page 11).

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

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

You are prompted for confirmation.

4 Click **Yes** in the confirmation dialog box to delete the user account.

5 You have completed this procedure.

—End—

Adding new groups

Application

Use this procedure to add new groups.

IEMS server allows group-based authorization.Different types of users are organized into groups. The group profile specifies a set of common operations that can be performed by the users in that group. Group-based authorization saves time in creating and managing users and their associated operations in IEMS.

Action

Step **Action**

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to ""Starting the Security Administration tool" (page 11)".

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.

The Groups Wizard window opens.

3 Enter the Group Name and the Group ID in the respective fields.The group ID is a unique numerical identifier for the group defined for the IEMS devices.

The group name cannot be longer than 8 characters.

The group name must consist of lower case alphabets or digits. The first character of a group name must be a lower case alphabet.

If a group ID field is not filled, then it is auto generated for the created group by the system.

The following are group ID range restrictions:

- Solaris group(s) GID range: 0-99
- Carrier VoIP application group(s) GID range: 100-12100

- IEMS-generated custom group(s) GID range: 12101-14000
- Customer-managed group(s): 14001+

4 Click the **Next** button.

The Permissions window for the group opens.

5 Click 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).

6 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.

7 You have completed this procedure.

—End—

Changing the system account passwords on the central security server

Application

Use this procedure to change passwords and set their expiry status to "never expire" on the following system accounts in a single operation on the IEMS security server:

> administrator, ndsadmin, puser, dsameuser, amldapuser, replication manager

The system accounts listed above are application accounts used internally by the IEMS security server components. They are not user accounts and therefore cannot be used for actual user login.

ATTENTION
The passwords of the system accounts listed above are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, the password and expiry change procedures described in this section must be performed on both servers.

ATTENTION
The server automatically restarts if this procedure is performed on the active server and so it is recommended that this procedure is performed as a scheduled event.

ATTENTION
If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that all steps in this procedure are performed to avoid any outage to central security servers.

Prerequisites

To perform this procedure, you must have root user privileges.

Action

Step	Action
	At your workstation
1	Change the amadmin password for the NSS-SAML client on the active and inactive IEMS Security servers. For details, see "Changing the amAdmin password" (page 59).

2 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 server where IEMS resides

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Change to the directory where the change password script is located by typing:

```
cd /opt/nortel/applications/security/core_1.1.0/bin/
```

and pressing the Enter key.

7 To change the system account passwords on the active server, type:

```
./ ss_change_passwd.sh
```

and press Enter.

If you are performing this procedure in	Do
a simplex configuration	you have completed this procedure
a high availability (HA) configuration	go to the next step

8 Telnet to the inactive server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where IEMS resides

9 When prompted, enter your user ID and password.

10 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

11 When prompted, enter the root password.

12 Change to the directory where the change password script is located by typing:

```
cd /opt/nortel/applications/security/core_1.1.0/bin/
```

and pressing the Enter key.

13 To change the system account passwords on the inactive server, type:

```
./ ss_change_passwd.sh -local
```

and press Enter.

14 You have completed this procedure.

—End—

Changing the saml password on an SPFS-based central security client

Application

Use this procedure to change the saml password on an SPFS-based central security client.

Prerequisites

You need root user privileges to complete this procedure.

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

1 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 SPFS-based client server

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

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.

6 Enter the number next to the ‘Configuration’ option in the menu, and press the Enter key.

7 Enter the number next to the ‘Security Services Configuration’ option in the menu, and press the Enter key.

8 Enter the number next to the ‘PAM Configuration’ option in the menu, and press the Enter key.

9 Enter the number next to the ‘Central Security Client Configuration’ option in the menu, and press the Enter key.

10 Enter the number next to the ‘saml_passwd_conf’ option in the menu, and press the Enter key.

Example response

```
=== Executing "saml_passwd_conf
"Enter the SAML password (default:  s1isamadmin):
mypassword
**Confirm Settings**
SAML Password:  s1isamadmin
Enter ‘ok’ to commit changes
Enter ‘quit’ to exit
Enter anything else to re-enter settings
```

11 Confirm the settings by typing

`ok`

and pressing the Enter key.

Example response

```
Configure Password Successful
==="saml_passwd_conf" completed successfully
```

You have completed this procedure.

—End—

Changing the amAdmin password

Application

Use this procedure to change the amAdmin password. The amAdmin account is an application account used internally by the IEMS security server components. It is not a user account and thus cannot be used for actual user logins.

ATTENTION
Changing the amAdmin password disrupts any existing security sessions and so it is recommended that this procedure is performed as a scheduled event.

ATTENTION
Passwords are changed in client machines first and then on the server. This means that changing the password on the client machine will prevent further logins using centrally administered accounts until the password has been changed on the server. As such, it is recommended that passwords on clients running critical applications are changed last. This means that the unavailability of centrally administered accounts will exist for a shorter period of time on these clients.

ATTENTION
If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

ATTENTION
When you run the configure_nsssaml.sh script to set the NSSwitch SPI passwords and the is_passwd.sh to set the Identity server passwords, you must set the passwords to the same value.

Prerequisites

None

Action

Perform the following steps:

- On each remote NSS-SAML client (not located on an IEMS server), starting with the least critical, change the NSSwitchSPI password (step 1 through step 13).
- On the inactive IEMS security server, change the NSSwitchSPI password (step 14 through step 19).

- On the active IEMS security server, change the NSSwitchSPI and the Identity Server passwords (step 20 through step 26).

Step	Action

At your workstation

1 Telnet to the active remote NSS-SAML client by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where the NSS-SAML client 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 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgm
t/bin/configure_nsssaml.sh
-subcomponent password
```

and pressing the Enter key.

6 When prompted, enter the new password.

7 Telnet to the inactive remote NSS-SAML client by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where the NSS-SAML client resides

8 When prompted, enter your user ID and password.

9 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

10 When prompted, enter the root password.

11 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgm
t/bin/configure_nsssaml.sh
-subcomponent password
```

and pressing the Enter key.

12 When prompted, enter the new password.

13 Repeat step 1 through step 12 for each remote NSS-SAML client (not located on an IEMS server), starting with the least critical.

14 Log in to the inactive IEMS security server as root by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where the IEMS security server resides

15 When prompted, enter your user ID and password.

16 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

17 When prompted, enter the root password.

18 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgm
t/bin/configure_nsssaml.sh
-subcomponent password
```

and pressing the Enter key.

19 When prompted, enter the new password.

20 Telnet to the active IEMS security server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where the IEMS resides

21 When prompted, enter your user ID and password.

22 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

23 When prompted, enter the root password.

24 Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgm
t/bin/configure_nsssaml.sh
-subcomponent password
```

and pressing the Enter key.

25 When prompted, enter the new password.

26 Change the Identity server password to the same value as the NSSwitch SPI password by entering:

```
/opt/nortel/applications/security/cur-
rent_isclient/bin/is_passwd.sh -is_passwd write
-exp <n>
```

where

n is the number of days after which the password for the amadmin account will expire. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

27 When prompted, enter the new password.

28 Enter the new password again.

29 You have completed this procedure.

—End—

Managing the certificate list for expiration monitoring

Application

Use this procedure to view the list of certificates to be monitored by the system, and to manage the list of certificates to be monitored by the system.

Prerequisites

You need root user privileges to complete this procedure.

Action

Step Action

At your workstation

1 Log in to the client server by typing:

```
> telnet server
```

and pressing the Enter key.

where

where

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

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

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Application Configuration
4 - CORBA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Disk Drive Replacement
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the Security Services Configuration option in the menu.

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet,
snmp and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - Password Monitor Configuration
11 - Certificate Monitor Configuration
12 - Register Certificate for Monitoring
13 - query_registry (Query Network Services Package
Registration)
14 - Change Password Encryption Key Length
x - exit
select -
```

8 Enter the number next to the Register Certificate for Monitoring option in the menu..

Example response

```
Register Certificate for Monitoring
1 - List Certificate (list Certificate)
2 - Add Certificate (Add Certificate)
3 - Delete Certificate (Delete Certificate)
4 - List Certificate Alias (list Certificate alias)
X - exit
select -
```

9 Select your next step.

If you want to	do
list a certificate to be monitored	the next step
add a certificate to the monitor list	step 12
remove a certificate from the monitor list	step 14
List a certificate alias	step 16

10 To list a certificate to be monitored, enter the number next to the List Certificate option.

Example response

```
===Executing List Certificate
NOTE: list certificate in keystore
Enter Certificate alias name (default:)  verisignclass
2ca
**Confirm Settings** Certificate name(alias):
verisignclass2ca
Enter ok to commit changes
Enter quit to exit
Enter anything else to re-enter settings ok
verisignclass2ca /tmp/verisignclass2ca.crt admin@loca
lhost.com 0
verisignclass3ca /tmp/verisignclass2ca.crt admin@loca
lhost.com 0
verisignclass4ca /tmp/verisignclass2ca.crt admin@loca
lhost.com 0
verisignclass2ca, May 1, 2006, trustedCertEntry,
Certificate fingerprint (MD5):  B3:9C:25:B1:C3:2E:32:5
3:80:15:30:9D:4D:02:77:3E
NOTE: Successfully retrieved certificate from keystore.
===List Certificate execution completed
```

11 You have completed this procedure.

12 To add or register a certificate to the monitor list, enter the number next to the Add Certificate option. The certificate to be monitored is stored in a persistent JKS keystore. JKS keystore handles X.509 certificates. Other formats of certificate must be converted first to enable registration.

Example response

```
===Executing Add Certificate
NOTE: add certificate in keystore
Enter Certificate alias name (default:  )  verisigncl
ass2ca
Enter Certificate file name (default:  ):/tmp/verisignc
lass2ca.crt
Enter administrator email address (default:  ):<email
address>
**Confirm Settings**
Certificate name(alias):  verisignclass2ca
Certificate file name:  /tmp/verisignclass2ca.crt
Administrator email address:  <email address>
Enter ok to commit changes
Enter quit to exit
Enter anything else to re-enter settings ok
Certificate was added to keystore
NOTE: Successfully add certificate to keystore.
===Add Certificate execution completed
```

13 You have completed this procedure.

14 To remove a certificate from the monitor list, enter the number next to the Delete Certificate option.

Example response

```
===Executing Delete Certificate
NOTE: delete certificate in keystore
Enter Certificate alias name (default:)  verisignclass
2ca
**Confirm Settings**
Certificate name(alias):  verisignclass2ca
Enter ok to commit changes
Enter quit to exit
Enter anything else to re-enter settings ok
NOTE: Successfully delete the certificate from
keystore.
===Delete Certificate execution completed
```

15 You have completed this procedure.

16 To list the certificate alias, enter the number next to the List Certificate Alias option in the menu.

Example response

```
  === Executing List Certificate Alias
NOTE: list certificate alias in keystore
registered alias:
verisignclass2ca
verisignclass3ca
verisignclass4ca
===List Certificate alias execution completed
select -
```

17 You have completed this procedure.

—End—

Changing the password warning threshold on the central security server

Application

Use this procedure to change the system-wide password warning threshold for user accounts managed by the IEMS Security Server.

The new system-wide password warning threshold takes effect when passwords of existing user accounts are reset or when new user accounts are created.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Step **Action**

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 server where IEMS 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 Change to the directory where the global password warning script is located by typing:

```
/opt/nortel/applications/security/current_s1isext/sw
mgmt/bin
```

and pressing the Enter key.

6 Run the global password warning script by typing:

```
./updateGlobalPasswdWarning.sh
```

and pressing the Enter key.

7 When prompted, enter the number of days you want to set. Press the Enter key.

8 You have completed this procedure.

—End—

Upgrading the system password encryption

Application

Use this procedure to enhance encryption key management capabilities used for symmetric key cryptography. The encryption key can be used to encrypt or decrypt the passcode for certificates, system account passwords, and SNMP community strings.

By default, the Java Cryptography Extension (JCE) jurisdiction policy files offered by JDK 5.0 allows cryptography using the Advanced Encryption Standard (AES) with Electronic Codebook (ECB) mode and 128-bit keylength encryption. Where not restricted by export control, you can use a higher keylength of 192 or 256 bit by installing unlimited jurisdiction policy files. Subsequent encryption or decryption is then carried out using the configured key length. The key itself is not replaced.

Prerequisites

You need root user privileges to complete this procedure.

Action

Step Action

At your workstation

1 Download the unlimited strength version of the JCE jurisdiction policy files from the following link: http://java.sun.com/products/jce/javase.html#UnlimitedDownload

2 Install the JCE jurisdiction policy files. Refer to the README file that is included in the download package for instructions. Note that the security services home directory for JCE is as follows:

```
/opt/nortel/3rd_party/java/current_jre
```

3 To change the strength of the key form the default 128 bit to 192 or 256 bit, telnet to the active IEMS security server by typing:

```
> telnet server
```

and pressing the Enter key.

where

where

`server` is the IP address or host name of the server where the IEMS security server resides

4. When prompted, enter your user ID and password.

5. Change to the root user by typing:

   ```
   $ su - root
   ```

   and pressing the Enter key.

6. When prompted, enter the root password.

7. 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 -
   ```

8. Enter the number next to the Configuration option in the menu.

   Example response

   ```
   Configuration
   Configuration
   1 - NTP Configuration
   2 - Apache Proxy Configuration
   3 - OAMP Application Configuration
   4 - CORBA Configuration
   5 - IP Configuration
   6 - DNS Configuration
   7 - Syslog Configuration
   8 - Remote Backup Configuration
   9 - Database Configuration
   10 - NFS Configuration
   11 - Bootp Configuration
   12 - Restricted Shell Configuration
   13 - Security Services Configuration
   14 - Disk Drive Upgrade
   15 - Disk Drive Replacment
   16 - Login Session
   17 - Location Configuration
   18 - Cluster Configuration
   19 - Succession Element Configuration
   20 - snmp_poller (SNMP Poller Configuration)
   21 - backup_config (Backup Configuration)
   X - exit
   Select -
   ```

9 Enter the number next to the Security Services Configuration option in the menu.

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet,
snmp and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - Password Monitor Configuration
11 - Certificate Monitor Configuration
12 - Register Certificate for Monitoring
13 - query_registry (Query Network Services Package
Registration)
14 - Change Password Encryption Key Length
x - exit
select -
```

10 Enter the number next to the Change Password Encryption Key Length option in the menu.

Example response

```
Enter the number next to the “Change Password
Encryption Key Length” option in the menu.
Example response === Executing “change password
encryption key length”
1 -
NOTE: changing the key length in key file
Enter Certificate alias name (128|192|256):
** Confirm Settings
** New key length to set:
Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings ok
```

11 Enter the key length and enter OK to change the key length.

12 Change the password encryption by entering:

```
/opt/nortel/applications/security/current_isclient/bin/
is_passwd.sh -local write <is_passfile>
```

where

is_pass file is the name of the password file where the newly encrypted password will be written to.

13 You have completed this procedure.

—End—

Fine-grained access control using custom scopes

There are two types of scope that the IEMS administrator can configure to manage viewing of objects or access to operations.

- To customize views, the IEMS administrator can perform the following custom view scope tasks:
  - "Adding a custom view scope to a group" (page 80)
  - "Assigning a custom view scope to a group" (page 83)
  - "Setting custom view scope properties" (page 85)
  - "Deleting a custom view scope from a group" (page 92)

  For more information about custom view scopes and a use case example, see "Custom view scopes" (page 76).
- To manage authorization to perform operations, the IEMS administrator can perform the following authorization scope tasks for an operation within a user group:
  - "Adding an authorized scope to an operation" (page 93)
  - "Changing an authorized scope for an operation in a group" (page 95)
  - "Deleting an authorized scope from a group operation" (page 96)

  For more information about authorization scopes and a use case example, see "Authorized scopes for operations" (page 77).

The IEMS administrator can also perform the following group configuration tasks:

- "Assigning a user to a group" (page 97)
- "Assigning operations to a group" (page 99)

Custom view scopes

Regionalization or network partitioning-based access control can be managed through custom view scopes which are attached to user groups.

A custom view scope is a restricted customized view which only displays objects related to the set of users or a group based on the configured scope criteria. The custom view scope can be used to filter information so that users can only view the data on which they are authorized to perform operations.

For example, in a network management environment, where one group of users is authorized to access the nodes in Network A, and another group of users is authorized to access the nodes in Network B, all users are likely to use the same user interface but with different authorized areas or network nodes. A Network B user will not be able to manage or unmanage nodes on Network A, because he does not have authorization to perform tasks on Network A nodes. Therefore, it is necessary to customize the view for each group and to provide the groups with a view of nodes where they are authorized to perform tasks.

Example
To provide the groups with a view of the nodes where they are authorized to perform tasks, do the following:

- Create an authorized scope with the following property values:

  ```
  parentNet="IP address of Network B"
  ```

  For details on how to add an authorized scope, see "Adding an authorized scope to an operation" (page 93).

- Create a custom view scope.

  For details on how to create a custom view scope, see "Adding a custom view scope to a group" (page 80).

- Assign the authorized scope to the custom view scope.
- Assign the authorized scope to the respective group of users who have their permissions already set to perform manage/unmanage objects operations.

This gives the Network B user a view of the nodes which have a parent network value of <IP address of Network B> and on which he can perform operations.

IEMS has five scopes under which the IEMS administrator can set properties. The modules are as follows:

- Topology (Maps)
- Events
- Alerts

- Inventory (Network Database)
- Stats Admin

  Custom view scopes cannot be added to the standard Carrier Voice over IP user groups.

Example use cases for custom view scopes for groups

The following are examples of how custom view scopes can be used.

Example
To create a custom scope view to view devices with a display name beginning with GWC in subnet 47.1.123.1, do the following:

- Create a custom view scope using the Topology module.

  For details on how to create a custom view scope, see "Adding a custom view scope to a group" (page 80).

- In the Scope Settings window, set the following rules:

  ```
  displayName=GWC*
  ```

  ```
  IPaddress=47.1.123.1
  ```

Example
To create a custom view scope to display events that start with IEMS as a LogKey property, do the following:

- Create a custom view scope using the Events module.

  For details on how to create a custom view scope, see "Adding a custom view scope to a group" (page 80).

- In the Scope Settings window, set the following:

  ```
  LogKey=IEMS*
  ```

Example
To display performance collection data for all components except for GWC, do the following:

- Create a custom view scope using the Stats Admin module.

  For details on how to create a custom view scope, see "Adding a custom view scope to a group" (page 80).

- In the Scope Settings window, set the following:

  ```
  Agent=!GWC*
  ```

Authorized scopes for operations

Resource-based access control can be managed through authorized scopes which are attached to one or more operations in a group.

An authorized scope stores authorization information and can be used to restrict access for users to perform specific tasks within an operation. An authorized scope consists of an authorized scope name and a set of properties. To manage user access, you define properties for the authorized scope and assign the scope to the user’s group.

For example, a user who has permission to perform the "manage and unmanage objects" operation has access to manage any node or network. The IEMS administrator can restrict the permission of the user in order to manage specific nodes or networks only. The IEMS administrator can do this by setting property values for the authorized scope for the "manage and unmanage objects" operation and assigning the authorized scope to the user’s group.

Example
If you want the user to have access to the network 123.12.1.3 and SNMP nodes only, do the following:

- Select the user group to which the user belongs in the Security Administration tool in the IEMS Java Web Client.
- Select the "manage and unmanage object" operation.
- Set the following property values.

```
propertyName="type",propertyValue="snmpNode"
propertyName="network",propertyValue="123.12.1.3"
```

For details on adding and modifying authorized scopes, see "Adding an authorized scope to an operation" (page 93) and "Changing an authorized scope for an operation in a group" (page 95).

Example use cases for authorization scopes for operations

The following are examples of how authorization scopes can be used.

Example
To authorize a user to have access only to edit the topology for network 47.1.123.1, do the following:

- Select the user group to which the user belongs.
- Select Map Editing Operations for the group.
- In the Scope Settings window, set the following property value:

```
propertyName="network",propertyValue="47.1.123.1"
```

Example
To authorize a user to view logs for SNMP nodes only, do the following:

- Select the user group to which the user belongs.
- Select the View Logs operation for the group.

- In the Scope Settings window, set the following property values:

```
propertyName="network",propertyValue="snmpNode"
```

Example
To authorize a user to manage events with a severity of critical, do the following:

- Select the user group to which the user belongs.
- Select Event User Operations for the group.
- In the Scope Settings window, set the following property value:

```
propertyName="severity",propertyValue="critical"
```

Adding a custom view scope to a group

Application

Use this procedure to add a new custom view scope to an existing non Carrier Voice over IP group using one of the following custom view scopes:

- Topology (Maps)
- Events
- Alerts
- Inventory (Network Database)
- Stats Admin

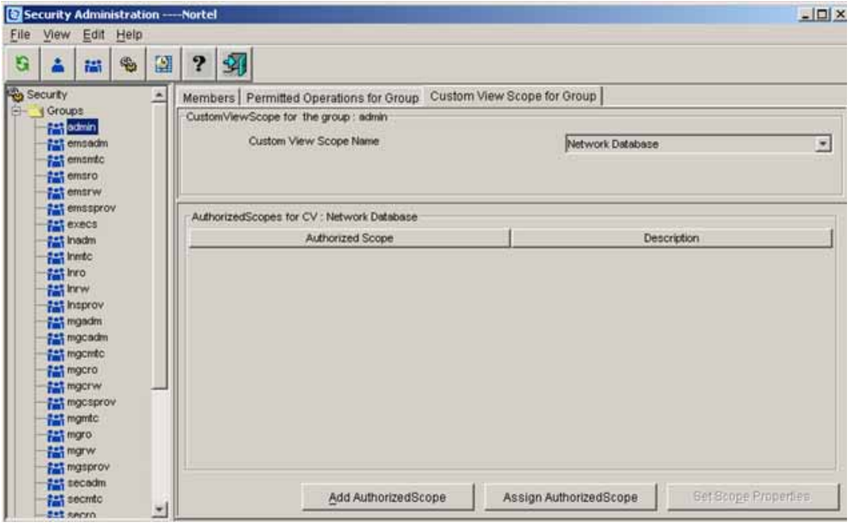
For a description of custom view scopes, refer to "Fine-grained access control using custom scopes" (page 75).

Prerequisites

You must have administration privileges to perform this procedure.

Action

Step	Action
At the IEMS workstation	
1	Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).
2	Select the group for which you want to set a scope under the Groups node in the Security tree.
3	Select the **Custom View Scope for Group** tab to display all the custom view scopes for the selected group. *A window similar to the following opens.*



CustomViewScope for the group : admin

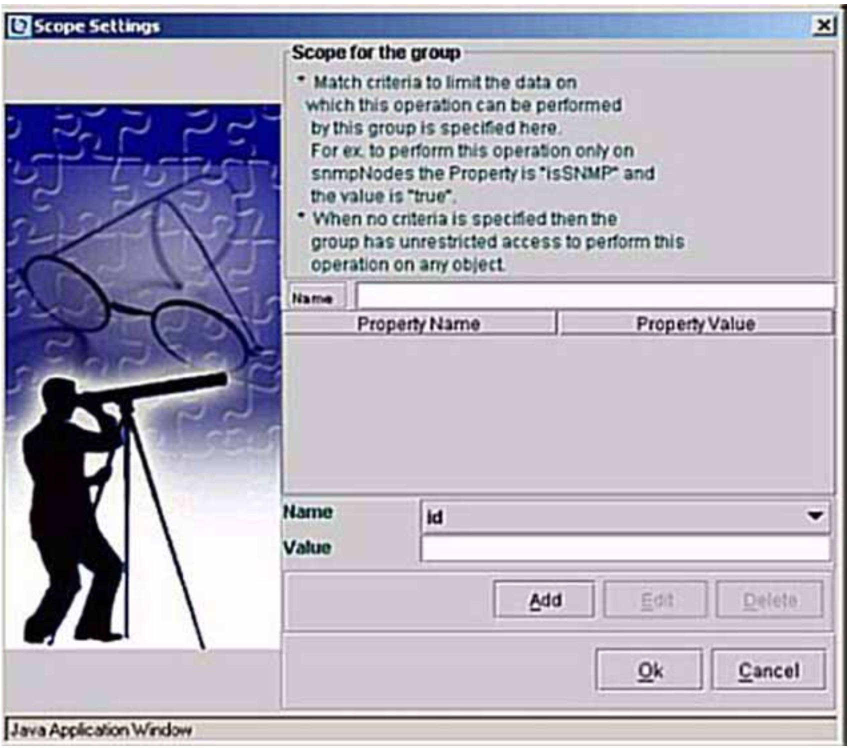
Custom View Scope Name: Network Database

AuthorizedScopes for CV : Network Database

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

5 Click the **Add AuthorizedScope** button.

A window similar to the following opens.



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: id

6 Enter a name for the custom view in the Name field.

7 Select a property name from the Name drop-down menu. For details of the property names and values for the custom view scopes, see "Properties and values of custom view scopes" (page 87).

8 Enter the value for the property in the Value field. For details of how to set property values, see "Setting custom view scope properties" (page 85).

9 Click the **Add** button to add the selected properties to the selected custom view scope.

10 Click the **OK** button to update scope details in the IEMS Server.

11 You have completed this procedure.

—End—

Assigning a custom view scope to a group

Application

Use this procedure to assign a custom view scope to a group.

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

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to ""Starting the Security Administration tool" (page 11)").

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

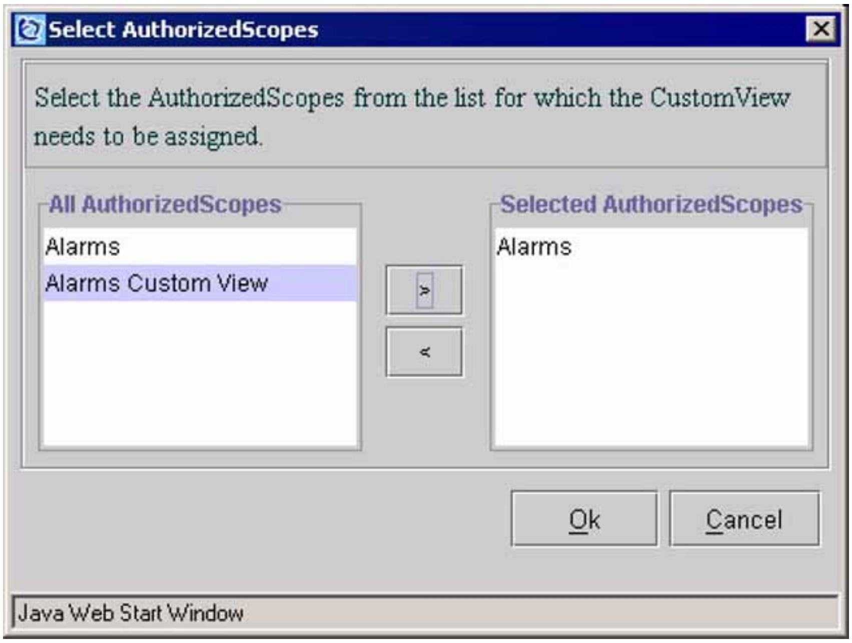
3 Click the **Custom View Scope for Group** tab in the right-hand panel.

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

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 IEMS Server.

8 You have completed this procedure.

—End—

Setting custom view scope properties

Application

Use this procedure to set custom view scope properties.

The IEMS administrator can set the properties of the custom view scope. For more information on custom view scopes, see "Fine-grained access control using custom scopes" (page 75).

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to ""Starting the Security Administration tool" (page 11)").

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

This displays 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 button.*

4 Click the **Set ScopeProperties** button.

The Scope Settings dialog is displayed.

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

6 Specify the set of wild card characters that are supported in IEMS 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*.

Operator	
!(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*.
, (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.

7 You have completed this procedure.

—End—

Properties and values of custom view scopes

The property names used for each scope are listed in the table "Custom view scopes and their associated property values" (page 87).

Click on the following links to view the property value details:

- "Property values for the Topology (Maps) and Inventory (Network Database) custom view scopes" (page 88)
- "Property values for the Event custom view scopes" (page 89)
- "Property values for the Alert custom view scopes" (page 90)
- "Property values for the Stats Admin custom view scopes" (page 91)

Custom view scopes and their associated property values

Custom view scope	Property name
Topology (Maps)	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress, emIPAddress
Events	id, text, category, severity, time, source, node, logName, logNumber, logKey, sequenceNumber, eventLabel, eventType, componentId, probableCause, specificProblem, equipmentIdentifier
Alerts	entity, id, message, category, severity, modTime, createTime, who, source, logName, logNumber, logKey, sequenceNumber, eventLabel, eventType, componentId, probableCause, specificProblem, equipmentIdentifier
Inventory (Network Database)	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress, emIPAddress
Stats Admin	name, id, agent, oid, threshold, isMultiplePolledData, numericType, previousSeverity, statsDataTableName, protocol, dnsName, lastTimeValue

The following tables list the details of the property values for each scope.

Property values for the Topology (Maps) and Inventory (Network Database) custom view scopes

Property name	Property value
name	Displays the name or unique key for the object
displayName	Displays the name assigned to the device which was added to the IEMS
managed	True - device is managed False - device is not managed
status	1 - Critical 2 - Major 3 - Minor 4 - Warning 5 - Clear 6 - Info 7 - Unknown
isContainer	Indicates that the ManagedObject class uses the ContainerInterface
ipAddress	Displays the IP address of the device added to the IEMS
primaryIpAddress	Displays the IP address of the active unit (Unit 0) for duplex devices
secondaryIpAddress	Displays the IP address of the inactive unit (Unit 1) for duplex devices
timeZone	Displays the time zone associated with the object
deviceVersion	Displays the version of the device added to the IEMS
FIState	Displays the fault interface state of the managed object
SystemUnmanageState	Displays the system unmanage state. If the managed object is in the Throttle_Unmanaged state for the specified throttle state count, the fault interface state for this device changes to system_unmanage.

Property name	Property value
platformAddress	Displays the platform address
emIPAddress	Displays the IP address of the element manager added to the IEMS

Property values for the Event custom view scopes

Property name	Property value
id	Displays the unique ID of the event object
text	Displays descriptive text about the event
category	Displays the category of events
severity	1 - Critical 2 - Major 3 - Minor 4 - Warning 5 - Clear 6 - Info 7 - Unknown
time	Displays the time of the event
source	Displays information about the source of the event
node	Displays the node which generated the event
logName	Displays the generated log name
logNumber	Displays the generated log number
logKey	Displays a combination of the log name and log number
sequenceNumber	Displays the sequence number of the event
eventLabel	Displays the label for the event
eventType	Displays the type of event
componentId	Displays the component ID
probableCause	Displays the cause of the event

Property name	Property value
specificProblem	Displays a description of the problem for the event
equipmentIdentifier	Displays the identifier of the devices added to the IEMS (for example, displays the IP address of the device)

Property values for the Alert custom view scopes

Property name	Property value
entity	Displays the entity where the alert occurred
id	Displays the id of the event from which the alert is generated or last updated
message	Displays additional information about the alert
category	Category of alerts
equipmentIdentifier	Displays the identifier of the devices added to the IEMS (for example, displays the IP address of the device)
severity	1 - Critical 2 - Major 3 - Minor 4 - Warning 6 - Info 7 - Unknown
modTime	Displays the date and time when the alert was last modified
createTime	Displays the date and time when the alert was created
who	Displays the user who acknowledged the alert
source	Displays information about the source of the alert
logName	Displays the log name
logNumber	Displays the log number
logKey	Displays a combination of the log name and log number
sequenceNumber	Displays the sequence number
eventLabel	Displays the event label
eventType	Displays the event type

Property name	Property value
componentId	Displays the name of the component that raised the alert
probableCause	Displays the cause of the event
specificProblem	Displays a description of the problem for the alert

Property values for the Stats Admin custom view scopes

Property name	Property value
name	Displays the name of the job
agent	Displays the name of the component for which collection is enabled
dnsName	Displays the DNS name
id	Displays the poll ID
protocol	Displays the protocol
numericType	1 - numeric 2 - string
previousSeverity	Displays the previous severity of the polled data
statsDataTableName	Displays the table where the collected data is stored
oid	Displays the object data identifier
threshold	True - threshold value set for data collection False - threshold value not set for data collection
isMultiplePolledData	True - multiple polled data is enabled False - multiple polled data is not enabled
lastTimeValue	Displays the time at which the last value was collected

Deleting a custom view scope from a group

Application

Use this procedure to delete an authorized scope associated with a custom view scope from the database. For more information on custom view scopes, see "Fine-grained access control using custom scopes" (page 75).

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).

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.

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.

7 You have completed this procedure.

—End—

Adding an authorized scope to an operation

Application

Use this procedure to add a new authorized scope to an existing group. For a description of an authorized scope, refer to "Fine-grained access control using custom scopes" (page 75).

Prerequisites

You must have administration privileges to perform this procedure.

Action

Step Action

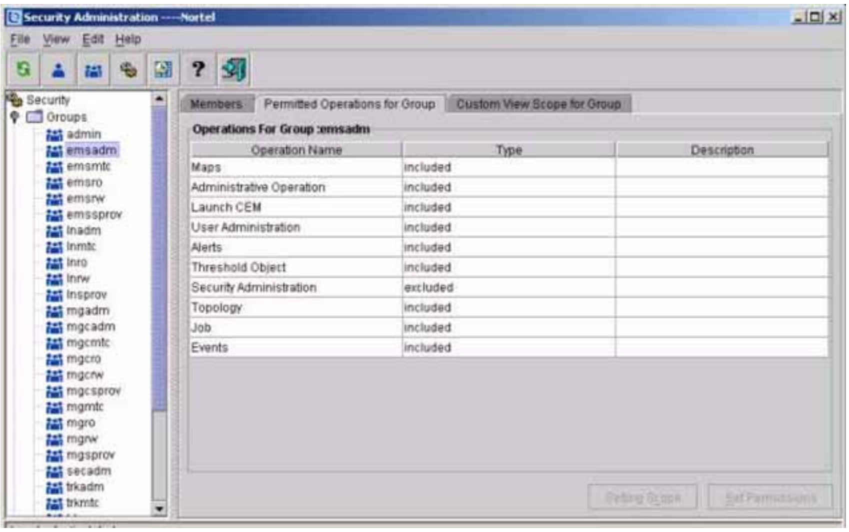
At the IEMS workstation

1 Launch the Security Administration tool (refer to the ""Starting the Security Administration tool" (page 11)").

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 :emsadm

Operation Name	Type	Description
Maps	included	
Administrative Operation	included	
Launch CEM	included	
User Administration	included	
Alerts	included	
Threshold Object	included	
Security Administration	excluded	
Topology	included	
Job	included	
Events	included	

The meaning of the Type values is as follows:

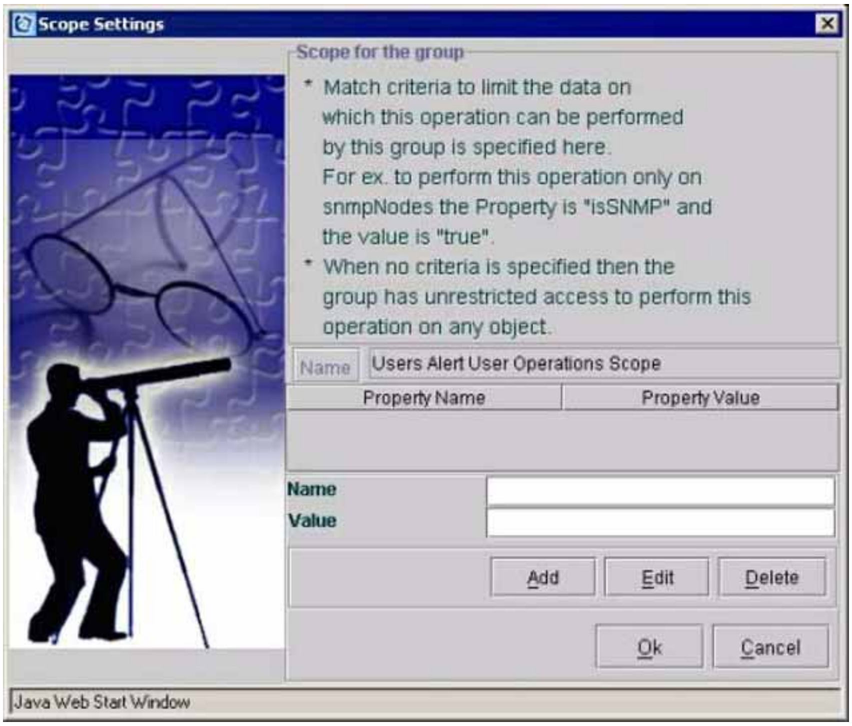
- included - the operation is an authorized operation of the view

- 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

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

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 IEMS Server.

9 You have completed this procedure.

—End—

Changing an authorized scope for an operation in a group

Application

Use this procedure to modify the scope for the group.

For a description of authorized scopes, refer to "Fine-grained access control using custom scopes" (page 75).

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to the ""Starting the Security Administration tool" (page 11)").

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 IEMS Server.

9 You have completed this procedure.

—End—

Deleting an authorized scope from a group operation

Application

Use this procedure to delete an authorized scope from a group operation.

You can delete an existing scope for the group. For a description of an authorized scope, refer to "Fine-grained access control using custom scopes" (page 75).

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool (refer to the ""Starting the Security Administration tool" (page 11)").

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 IEMS server.

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.

9 You have completed this procedure.

—End—

Assigning a user to a group

Application

Use this procedure to assign a user to a group.

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

You can add local user accounts on the SPFS-based server and assign groups using the procedure in "Setting up local user accounts on an SPFS-Based Server" (page 158).

Action

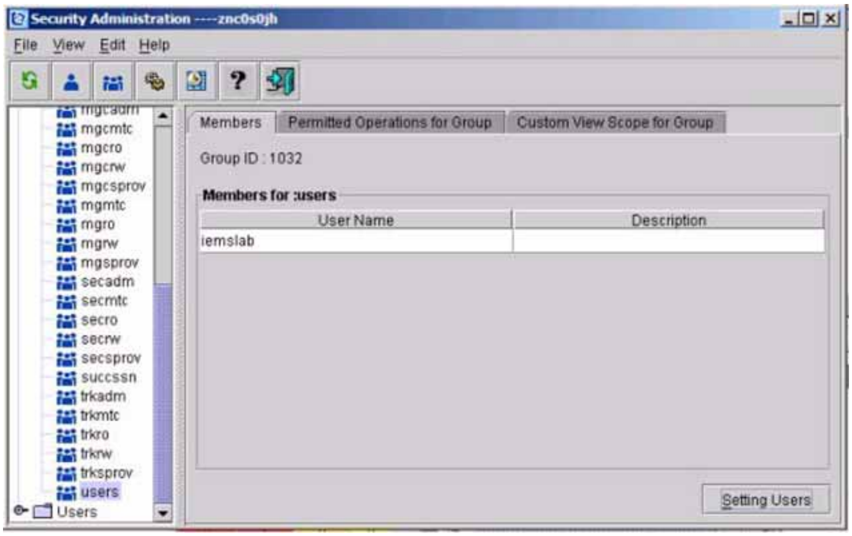
Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to "Starting the Security Administration tool" (page 11).

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.



Security Administration ----znc0s0jh

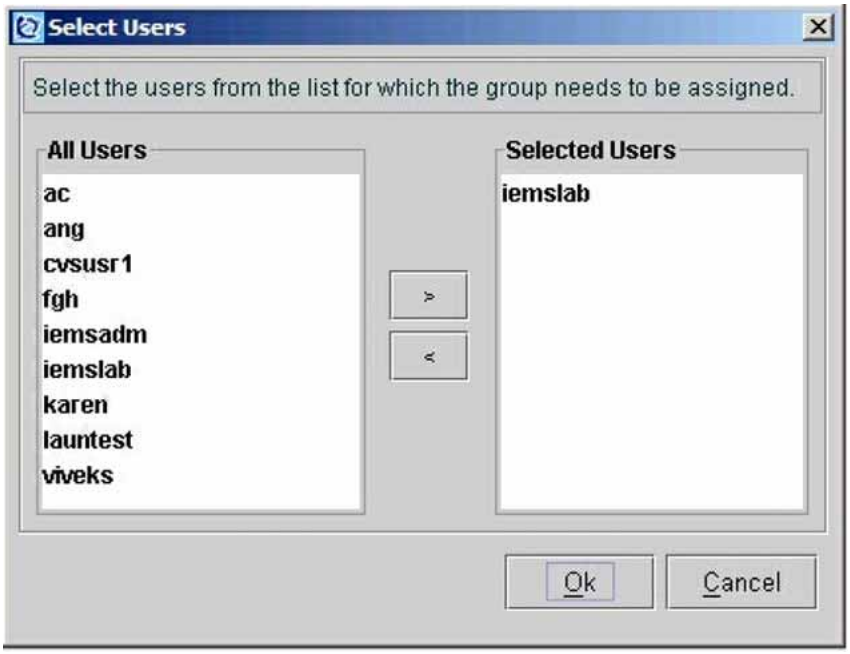
Group ID : 1032

Members for :users

User Name	Description
iemslab	

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.

All Users: ac, ang, cvsusr1, fgh, iemsadm, iemslab, karen, launtest, viveks

Selected Users: iemslab

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.

The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in IEMS and groups created at the SPFS / Sun Solaris level.

6 Click the **OK** button to update the changes in the IEMS server.

7 You have completed this procedure.

—End—

Assigning operations to a group

Application

Use this procedure to assign operations to a group.

In IEMS, by default, operations are assigned to the 33 Carrier VoIP groups. The administrator cannot assign any specific operation to these existing groups but can assign operations to any newly added group in the IEMS.

The list of operations that are privileged for the **admin** group are:

S. No:	Operation
1	Administrative Operations
2	Events
3	Topology
4	Job
5	User Administration
6	Alerts
7	Configuration
8	Maps
9	Threshold Object
10	Launch
11	Radius Secrets Operation

Action

Step Action

In the Security Administration tool of IEMS

1 Launch the Security Administration tool. Refer to ""Starting the Security Administration tool" (page 11)".

2 Select the group (other than the existing groups) 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.

The Assign Permissions dialog box opens.

5 Click 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 (these operations inherit the parent operation’s permission).

6 Click the **Done** button to update the operation details in the IEMS server.

7 You have completed this procedure.

—End—

Using the Operations tree

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

Setting user permissions for operations

Application

Use this procedure to launch the Operations dialog and to set permissions for the following user operations:

- Administrative Operation
- Events
- Topology
- Job
- User Administration
- Configuration
- Alerts
- Maps
- Threshold Object
- Polling Units
- Domain
- Launch
- Radius Secrets Operation

Action

Step	Action
	In the Security Administration tool of IEMS
1	Launch the Security Administration tool. Refer to ""Starting the Security Administration tool" (page 11)" for more details.
2	In the Security tree, expand the users node and select the user whose operations you want to modify.
3	Select the **Permitted Operations for User** tab.
4	Click the **Set Permissions** button. *The Operation Tree Configuration dialog box opens.*
5	Click 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 (these operations inherit the parent operation’s permission).

6 You have completed this procedure.

—End—

The following table provides descriptions of the operations that you can add or remove in the Operation Tree Configuration dialog box:

Description of operations in the Operations Tree Configuration dialog box

Operation	Description
Administrative Operation	
Security Administration	Security Management is used to authenticate a user to log into IEMS and provide permissions to perform certain operations.The operations under this category are as follows: • Group Operations: For adding, removing, and assigning permissions to groups of IEMS. • Operation Settings: For creating and removing operations in the Operations tree. • Scope Settings: For adding a new scope or setting properties to a scope and for assigning a scope to a group in the Custom View Scope. • View Logs: For viewing the logs. • SNMP Templates: For creating templates for a data collection job.
Configure Log Levels	This operation can be used to set the logging and the corresponding levels for various modules in the IEMS server.
Runtime Administration	This operation is a powerful tool to configure the IEMS server settings from the IEMS without the need for the user to restart the server for the new settings to take effect.
System Administration	This operation is the entry point for all administrative operations.
Northbound Configuration	This operation is for configuring the northbound devices of IEMS.The following types of northbound configurations are supported: • SCC2 NB Config:This operation is for configuring SCC2 supported northbound devices. • NTSTD NB Config:This operation is for configuring NTSTD supported northbound devices. • SNMP NB Config: This operation is for configuring SNMP supported northbound devices.

Operation	Description
Events	
Event User Operations	This operation is for event-related user operations. Some of the user operations are as follows: • Save Events To File: For saving the selected events or the events displayed in the Events Panel. • Print Event View: For printing either the selected events or events displayed in the Events Panel.
Event Filters	This operation is for viewing and modifying the event filters. • Get Event Filters: For viewing the event filters present in the server. • Set Event Filter: For modifying the existing event filters or creating a new event filter.
Event Cleanup	This operation is for cleaning up events.
Topology	
Modify Object	This operation is for modifying the managed object from managed state to unmanaged state or from unmanaged state to managed state. • Manage And Unmanage Objects: for setting the management status of the object at run time
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.
Dump Inventory Details	This operation is used to collect the list of discovered devices from the topology database and print them in a text file.
Job	
Add Job	This operation is for creating a new job.
Update Policy	This operation is for modifying the IEMS policies or jobs.
Delete Job	This operation is for removing an existing job from the system.
User Administration	
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 user.
Remove User From Group	This operation is used to remove a particular user from a group.
Change Password	This operation is used to change the existing password for a 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 set operations or permissions for existing users.
Set User Profile	This operation is used to set profiles for existing users.

Operation	Description
Clear Audit Trails	This operation is used to clear audit trails for a user.
Configuration (used by the MS2000 Configuration and Maintenance tool)	
Security Config	Allows the user to enable/disable IPSec, configure IPsec, change the web interface login and password, change the SNMP passwords, setup SNMP trusted managers.
Reload Node	Allows the user to reload the node and backup INI files to the tftp server.
Node Maint	Allows the user to lock, unlock, backup the INI files to the IEMS server, and reset the node.
Change Config	Allows the user to change the non-security related fields on the node, including setting up where to route traps (trap destination tab).
Retrieve Config	Allows the user to launch and look at all of the screens in the MS2000 GUI.
Configure Platforms	This operation is used to configure platforms.
Alerts	
Alert Filters	Get Alert Filters - for viewing the alert filters present in the server. Set Alert Filters - for modifying existing alert filters or for creating a new alert filter.
Alert User Operations	Set Alert Annotation - for adding notes to an alarm. Get Alert Details - for viewing the details of an alarm. Save Alerts To File - for saving either the selected alarms or the alarms displayed in the current alarm panel to a file. Print Alert View - for printing either the selected alarms or the alarms displayed in the current alarm panel. Clear Alerts - for changing the alarm severity to Clear. Get Alert Annotation - for viewing an existing alarm annotation. Get Alert History - for viewing the alarm history. Alert Pickup - used to pick up the alarm. Delete Alerts - used to remove an alarm.
Maps	
Map Editing Operations	This operation is used to configure maps, such as the creation of new maps, customizing map hierarchy, map symbol layout, and map symbol renderers in IEMS.
Threshold Object	
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.

Operation	Description
Polling Units	
Add Polling Units	This operation is used to add polling units.
Remove Polling Units	This operation is used to remove polling units.
Modify Polling Units	This operation is used to modify polling units.
Get Polling Unit	This operation allows the user to view the properties of the polled data and to configure the threshold list against a polled data object.
Domain	
OTHERS	This allows the user to view the IEMS Manager icon in the topology.
EMS	This allows the user to add or view devices under the EMS domain.
MG	This allows the user to add or view devices under the MG domain.
LN	This allows the user to add or view devices under the LN domain.
TRK	This allows the user to add or view devices under the TRK domain.
MGC	This allows the user to add or view devices under the MGC domain.
Launch	
Launch TMM	This operation is used for launching the TMM client.
Launch CEM	This operation is used for launching the CEM client.
Launch LMM	This operation is used for launching the LMM client.
Launch SBRM	This operation is used for launching the SBRM client.
Launch Command Line	This operation is used for launching the command line.
Remote Ping	This operation is used for launching Remote Ping.
Remote TraceRoute	This operation is used for launching Remote TraceRoute.
Launch PK Manager	This operation is used for launching the Certificate Manager client.
Radius Secrets Operation	
Radius Secrets Operation	This operation is used to enable the operation for RADIUS clients.

Adding new operations

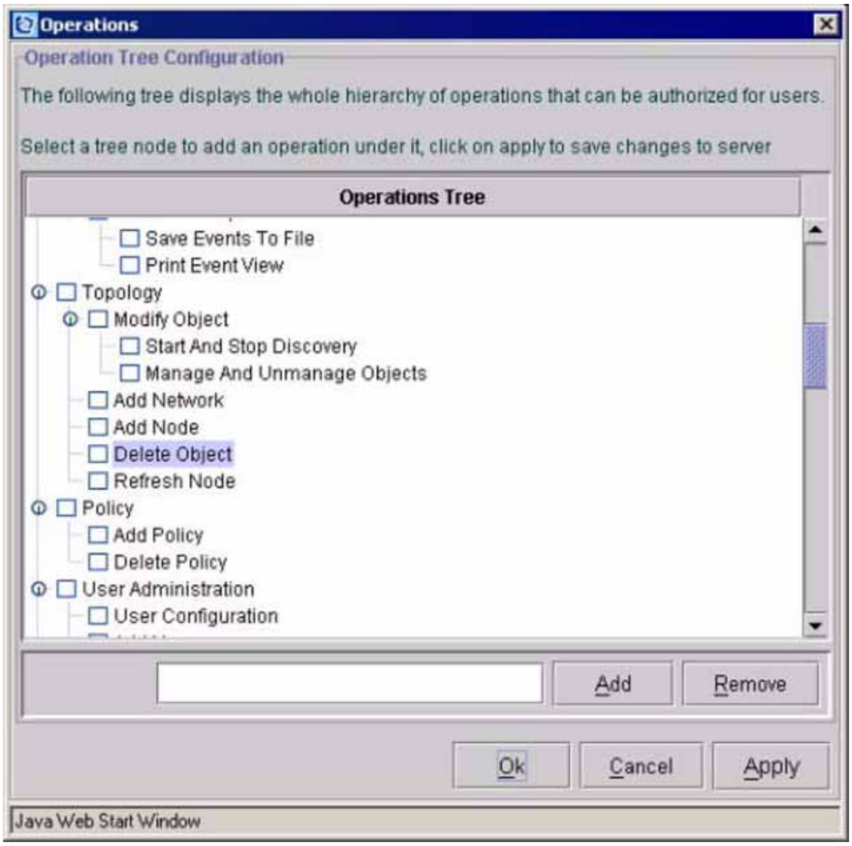
Application

Use this procedure to add a new operation to the Operations Tree.

A new application can be added to the IEMS. Once added, new operations can then be included for the (newly) added applications in the IEMS. For these operations to be authorized, they have to be present in the Operations dialog of the Security Administration tool.

Action

Step	Action
	In the Security Administration tool of IEMS
1	Launch the Security Administration tool (refer to ""Starting the Security Administration tool" (page 11)").
2	Select the **File-->New-->AddOperations** menu command. OR Click the **Operations** button in the toolbar. *The Operations dialog opens, as shown in the following figure*.



Operations

Operation Tree Configuration

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

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 IEMS Server.

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

8 You have completed this procedure.

—End—

Deleting an operation

Application

Use this procedure to delete an operation.

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

Action

Step	Action
	In the Security Administration tool of IEMS
1	Launch the Security Administration tool (refer to ""Starting the Security Administration tool" (page 11)").
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 IEMS Server. Alternatively click the **Apply** button to continue with other tasks in the Operations dialog.
5	You have completed this procedure.

—End—

Modifying login session timeouts on an SPFS-based server

Application

Use this procedure when you want to modify the login session timeouts for the following GUI and CLUI client applications:

- CS 2000 Management Tools GUI
- Network Patch Manager GUI and CLUI
- Line Maintenance Manager GUI
- Gateway Controller Manager GUI
- SAM21 Manager GUI
- Trunk Maintenance Manager GUI
- Batch Configuration Monitor GUI
- OSSGate CLUI
- Batch Provisioning Tool CLUI
- Audio Media Server CLUI
- Integrated Element Management System GUI

You can modify the following login session timeouts:

- user inactivity timeout, which specifies the amount of time a client session can be inactive before the user is required to log in again.
- user termination timeout, which specifies the amount of time a user has to log in again before the user is forced to exit the client session.

Both the user inactivity timeout and the user termination timeout have a default value of 10 minutes. If the default value is acceptable, you do not need to perform this procedure.

You can disable the timeout functionality in its entirety by setting the user inactivity timeout to 0, or only disable the user termination timeout by setting its value to 0.

For HA cluster systems, timeout values are set independently for each side of the cluster. If timeout values have only been changed on the active side of a cluster and a SWACT occurs, the timeout values will take the inactive side settings. To ensure consistent interface performance following a

SWACT, when a default timeout setting is changed on the active side of the cluster, the corresponding setting should also be changed on the inactive side of the cluster.

Prerequisites

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

Action

Perform the following steps to complete this procedure.

In a two-server configuration, you must perform this procedure on both the active and inactive servers.

Step Action

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 SPFS-based server, or the physical IP address of the active or inactive server in a two-server configuration.

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 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 -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

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

7 Enter the number next to the ‘Login Session’ option in the menu.

Example response

```
Login Session
 1 - login_session_timeout (User Inactivity
      Timeout Configuration)
 2 - login_session_termination (User
      Termination Timeout Configuration
 3 - login_session_reauthentication (User
      Reauthentication Disable Timeout
      Configuration)
 4 - login_session_server (Login Session Master
      Server Configuration)
 5 - telnet_greeting (Telnet Login Greeting)
 6 - login_retries (Login Retries Limit)
x - exit
select -
```

8 Use the following table to determine your next step.

If you want to modify the	Do
user inactivity timeout value	step 9
user termination timeout value	step 11

9 Enter the number next to the ‘login_session_timeout’ option in the menu.

Example response

```
===Executing "login_session_timeout"
Current value for Session Timeout is:
USER_INACTIVITY_TIMEOUT=10
export USER_INACTIVITY_TIMEOUT
Enter the Login Session Timeout Value in Minutes (0 ->
1440):
```

10 When prompted, enter the desired login session timeout value, or press the Enter key to accept the current value.

Specifying a value of 0 disables the timeout functionality in its entirety.

Example response

```
Modifying Login Session Timeout.
Done.
```

Proceed to step 11 if you want to change the login session termination timeout value, otherwise go to step 13.

11 Enter the number next to the ‘login_session_termination’ option in the menu.

Example response

```
===Executing "login_session_termination"
Current value for Session Timeout is:
USER_INACTIVITY_TIMEOUT=10
export USER_TERMINATION_TIMEOUT
Enter the Loging Session Termination Timeout Value in
Minutes (0 -> 1440):
```

12 When prompted, enter the desired login session termination timeout value, or press the Enter key to accept the current value.

Example response

```
Modifying Login Session Termination Timeout.
Done.
```

Specifying a value of 0 disables the login session termination timeout.

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.

You have competed this procedure.

—End—

Setting a limit for login retries on an SPFS-based server

Application

Use this procedure to set a limit on the number of login retries on a Server Platform Foundation Software (SPFS)-based server. When a user exceeds the number of login retries specified, the user loses connection to the host.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step Action

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 SPFS-based server on which you want to modify the login greeting

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 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 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Login Session" option in the menu.

Example response

```
Login Session
1 - login_session_timeout (User Inactivity Timeout
Configuration)
2 - login_session_termination (User Termination Timeout
Configuration)
3 - login_session_reauthentication (User Reauthenticat
ion Disable Timeout Configuration)
4 - login_session_server (Login Session Master Server
Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
X - exit
select -
```

8 Enter the number next to the "login_retries" option in the menu.

Example response

```
===Executing "login_retries"
Current value for Login Retries is:
```

```
RETRIES=3
Enter the Login Retries Limit Value (1->15):
```

9 When prompted, enter the limit value for login retries.

Example response

```
==="login_retries" completed successfully
```

Exceeding the range of the login retries limit value generates the error message "ERROR - Login Retries Limit Value Out Of Range", at which point you are prompted to enter a value between 1 and 15.

10 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Working with the centralized security server

Use this section to manage the centralized security server, as follows:

- Configure the IEMS central security server
- Configure an SPFS-based central security client
- Manage user accounts for central security
- Administer security tokens
- Administer health monitors
- Back up and restore of the central security server

Centralized security administration overview

IEMS provides centralized administration, authentication, authorization, and security logging for most components in the solution.

IEMS provides a pluggable security architecture based on the Pluggable Authentication Module (PAM) and Name Services Switch (NSS).

This architecture provides the following features:

- central administration of user accounts and user groups
- 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 IEMS 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.

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 IEMS central security server has been configured and activated in the network.

Central security administration - supported devices

Network element/EMS platform	Device authentication and authorization method	Documentation reference
USP	HTTPS	*USP Administration and Security*, NN10159-611
Ethernet Routing Switch 8600	RADIUS	*Configuring and Managing Security*, 314724-B
SPFS CS 2000 Management Tools Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager MG9000 Mid-Tier	PAM_RADIUS and NSS_SAML	*ATM/IP Solution-level Administration and Security*, NN10402-600
IEMS	HTTPS	*IEMS Administration and Security*, NN10336-611
CICM Manager	HTTPS	*CICM Configuration*, NN10240-511
Multiservice Data Manager (toolset)	PAM_RADIUS NSS_SAML	*MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements*, NN10180-612
Multiservice Data Manager (Operator Client)	SAML over HTTPS	*MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements*, NN10180-612
Media Gateway 7480/15000/20000	RADIUS	*MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements*, NN10180-612
Multiservice Switch 15000	RADIUS	*MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements*, NN10180-612
GWC	HTTP	No device-specific configuration needed

Network element/EMS platform	Device authentication and authorization method	Documentation reference
MG 9000	RADIUS	*MG 9000 Administration and Security*, NN10162-611
CS 2000 Core Manager (SDM)	PAM_RADIUS	*CS 2000 Core Manager Administration and Security*, NN10170-611

The following table lists IEMS single sign-on launch points.

IEMS single sign-on launch points

Network element/EMS platform/application	IEMS launch point
USP	USP Command Line USP Manager
CS 2000 Management Tools	CS 2000 Management Tools
GWC Manager	GWC Manager GWC Manager Network View GUI
SAM21 Manager	SAM21 Manager
UAS Manager	UAS Manager
LMM	LMM
TMM	TMM
OSSGate	BPT Servlet
MG9000 Manager MG9000 Mid-Tier	MG9000 Manager
APS	APS Manager APS Application
NPM	NPM
QOS	QOS Command Line
SPFS	SPFS Command Line (except CBM platform)
SDM platform	SDM 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 IEMS central security server to authenticate users and access user profile information.

IEMS 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 IEMS central security server in the network" (page 128).

When a request is forwarded to the IEMS PAM Service Provider (SPI), then authentication is performed against data provisioned and administered by the security administration application on the IEMS 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 in "Setting up local user accounts on an SPFS-Based Server" (page 158).

Customers can configure NSSwitch to use the service pre-bundled with IEMS 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 the IEMS security administration GUI. For details, see "Configuring a third-party Pluggable Authentication Module" (page 138).

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

Authorization domains

For the mapping details of IEMS devices to authorization domains, see "Mapping of IEMS devices to authorization domains" (page 25).

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 IEMS 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.

Media Gateway 7480/15000/20000, Multiservice Switch 15000, Ethernet Routing Switch 8600 and MDM do not support SSO.

Ports requirements

The following table lists details of port usage.

Process	Port Occupied	Communication
Performance (FTP or SFTP push)	Std.	TCP (out)
SSH	22	TCP (in)
TokenAdmin GUI and HTTPS Pam proxy (non-SSL mode)	80, 8080	TCP (in)
Trap Port	162 (default)	UDP (in and out)
TokenAdmin GUI and HTTPS Pam proxy (SSL mode)	443, 8443	TCP (in)
Syslog client	514	UDP (out)
LDAPS	636	TCP (in)
RADIUS server	1812	UDP (in and out)
SNMP Agent Port	8001 (default)	UDP (in)
Java Client Server Communication	9004, 9005	TCP (in)
NT STD Export	8555	TCP (in)
SCC2-Export Port	8556	TCP (in)
IEMS Server Web Server	9090 (default)	HTTP (in)
IEMS Server Web Server	9091 (default)	HTTPS (in)
IEMS Tomcat	18005, 18009	TCP (in)
SunONE IS (SSL mode)	58081	TCP (in)

Limitations and restrictions

The following are limitations and restrictions:

- the maximum number of provisionable central security users is 1000
- third party pluggability is supported for SunONE directory server 5.1 for LDAP
- for third party pluggability, the only pam.conf edits and the only nnswitch.conf edits that are supported are ldap. For details of pam_ldap edits, see "Configuring a third-party Pluggable Authentication Module" (page 138).
- password aging notification is not supported by the following:
  - — CICM Manager
  - — USP
  - — Ethernet Routing Switch 8600
  - — Media Gateway 7480/15000/20000
  - — Multiservice Switch 15000
  - — GWC
  - — MG 9000
- Central authentication for FTP is not supported as there is no local caching of user data on the local machine after authentication with a remote server.
- Centrex IP Client Manager (CICM) Element Manager 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 SPFS security clients
- a certificate must be installed on the IEMS server, before installing IEMS software, to ensure that the system operates correctly
- the total number of groups that a user can belong to cannot exceed sixteen
- a user name is a string of no more than eight bytes consisting of alphabetic characters and numeric characters. The first character

should be alphabetic, and the field should contain at least one lower case alphabetic character.

- a group name consists of characters from the set of lower case alphabetic characters and numeric characters
- IEMS allows you to configure user ID ranges. Sun Solaris security clients such as SPFS use a user ID to uniquely identify a user. The default IEMS user ID range is 10001-12000. You can change the IEMS user ID. You must ensure that there is no conflict between the new IEMS 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.

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, ntssg:50015, FIELD:50016, oracle:50017, patch:50018

- Media Gateway 7480/15000/20000, Multiservice Switch 15000, and MDM do not support SSO.
- User accounts provisioned in the Central Security Administration system:
  - — must not have the same numerical user ID or user name as user accounts provisioned in local Unix files on the IEMS server. If a conflict exists where a central user account has the same user name or numerical user ID as a local IEMS server account, then login with the central account may fail on some devices.
  - — can not have the same numerical group ID or group name as user groups provisioned in local Unix files on the IEMS Server. If a conflict exists where a central user group has the same group name or numerical group ID as a local IEMS group, then login involving the central user group may fail on some devices.
  - — For the reasons explained above, user/group names or numerical IDs among different security database systems should not have duplicate entries. The Carrier VoIP groups listed in the "Secondary user groups" (page 160) table are pre-defined by the IEMS Security Administration system and are an exception to this rule. The Carrier VoIP groups exist in both the IEMS server local Unix files and the Central Security Administrations system.
- When configuring /etc/nsswitch.conf for use with third party security modules, the saml nsswitch entry must always appear before the files

entry in the nsswitch stack. The following is an example of the password and group database entries:

Example
passwd: ldap saml files
group: ldap saml files

Configuring the IEMS central security server in the network

Application

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

ATTENTION
Only one IEMS 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 Server Platform Foundation Software (SPFS) must be performed to revert the security server to its previous configuration.

ATTENTION
User accounts managed by IEMS in previous releases will be automatically migrated from the IEMS Oracle database to the MFT NDS database when upgrading to IEMS (I)SN09.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated Element Management System (IEMS) is already installed or upgraded on the server, and it is running Server Platform Foundation Software (SPFS).
- an HTTPS certificate has been properly installed on the server prior to installing or upgrading the IEMS. If required, refer to procedure "Installing or replacing an HTTPS certificate on an SPFS-based server" (page 151). The Integrated security server and SunONE component will be automatically configured during installation or upgrade to enable the secure SSL mode.

Action

Perform the following steps to complete this procedure.

Step	Action
1	Delete the user accounts you want to add to the IEMS central security server.

a. Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

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

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

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

e. 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 want to migrate to the IEMS central security server.

2 If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts you want to centrally manage. If required, refer to ‘Adding new users’ in *IEMS Security and Administration*, NN10336-611.

If the central security administration application is a third-party application and not the IEMS, follow the procedures in the third party documentation

All users added through the IEMS Security Administration tool, are by default assigned to the "succssn" user group for login access.

3 Complete PAM and NSSwitch configuration as follows:

At installation or upgrade, the IEMS replaces the existing PAM and NSSwitch configuration files (pam.conf and nsswitch.conf) with new PAM and NSSwitch configuration files that use the IEMS security application. If the pam.conf or nsswitch.conf files had any special edits, you must re-edit the file to add those special edits.

You can use the IEMS PAM and NSSwitch SPIs, which are pre-bundled with the IEMS load, or you can use your own third-party PAM and NSSwitch SPIs. The Distributed Computing Environment (DCE) and the Lightweight Directory Access Protocol (LDAP) PAM and NSSwitch SPIs are the third-party PAM and NSSwitch SPIs that are supported. If required, refer to procedure "Configuring a third-party Pluggable Authentication Module" (page 138).

4 If necessary, add the SPFS platform to the IEMS topology. For an SPFS platform user account to be authorized, the SPFS platform must be a RADIUS client of the central security server. For details, see "Adding a Server Platform Foundation Software (SPFS) platform" in IEMS Configuration, NN10330-511.

If a centrally managed restricted access user account is created through the IEMS security application, then the home directory and profile are automatically created. In this case, you do not need to manually configure the user account for platform access.

5 You have completed this procedure.

—End—

Configuring an SPFS-based central security client

Application

Use this procedure to configure an SPFS-based central security client to use the Integrated Element Management System (IEMS) central security server.

> **ATTENTION**
> You can revert to the previous configuration of the client server using procedure Reverting the client server to its previous configuration.

In the event you want to reconfigure the central security client to use a new IEMS server IP, perform steps step 2 and step 3 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the IEMS central security server is already configured and activated in the network (see procedure "Configuring the IEMS central security server in the network" (page 128), if required)
- perform this procedure on each SPFS-based server that is not the IEMS central security server to activate centralized security

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

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

It is recommended to migrate all user accounts that exist on SPFS-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.

ATTENTION

It is strongly recommended to migrate all local user accounts (except the mentioned list above) to the IEMS central administration system. If local user accounts are not migrated, you have to ensure the local user name does not conflict with an IEMS central administration system user.

There is no way to prevent the creation of centralized accounts that are duplicates of local accounts that exist on the SPFS client machines. In the event that duplicate accounts are created, the IEMS account is used.

a. If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts plus any additional required user groups you want to centrally manage. If required, refer to "Adding new users", "Adding new groups", and "Assigning a user to a group" in *IEMS Security and Administration*, NN10336-611.

   All users added through the IEMS Security Administration tool, are by default assigned to the *succssn* user group for login access.

b. Delete the user accounts you just added to the IEMS central security server.

   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 SPFS-based client server

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

d. Change to the root user by typing

   ```
   $ su - root
   ```

   and pressing the Enter key.

e. When prompted, enter the root password.

f. 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 IEMS central security server.

2 Configure the IEMS security server address 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
X - Exit
select -
```

b. Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3- OAMP Application Configuration
4- CORBA Configuration
5- IP Configuration
6- DNS Configuration
7- Syslog Configuration
8- Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup 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
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
Select -
```

d. Enter the number next to the "Security Server Location Configuration" option in the menu.

   Example response

```
IEMS Server Location Configuration
1 - security_server_ip (Configure Security Server
IP)
x - exit
select
```

e. Enter the number next to the "security_server_ip" option in the menu.

   Example response

```
===Executing "security_server_ip"
Enter Server IP Address (default 0.0.0.0):
```

f. When prompted, enter the virtual IP address of the security server, or press the Enter key to accept the default value if one is specified.

   Example response

```
Enter Fully Qualified Domain Name (default :  no
default):
```

g. When prompted, enter the Fully Qualified Domain Name (FQDN) of the security server, or press the Enter key to accept the default value if one is specified.

   Example response

```
Server IP: 47.135.214.83
Fully Qualified Domain Name:  ca.nortel.com
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

h. Accept the IP address and FQDN you just entered by typing

   `ok`

and pressing the Enter key.

Example response

```
=== "security_server_ip" completed successfully
```

i. Return to the Security Services Configuration menu, by typing

`select -` **`x`**

and pressing the Enter key.

Response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
x - exit
select -
```

3 Configure PAM and NNSwitch SPI configuration as follows:

RADIUS client and RADIUS server should not be configured on the same box.

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)
3 - saml_passwd_conf (Configure saml password)
x - exit
select -
```

c. Enter the number next to the "pam_radius" option in the menu.

Example response

```
===Executing "pam_radius"
Activating pam radius components
Security Server IP: 45.12.23.56
Security Server Fully Qualified Host Name:
test3iems.us.nortel.com
Enter the Shared Secret (default:  nortelnetworks):
```

d. When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.

   Example response

   ```
   Enter Radius Client Timeout (default:  12):
   ```

e. When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

   Example response

   ```
   Enter SAML Connection Timeout (default:  20):
   ```

f. When prompted, enter the SAML connection timeout (used to establish SAML connections with the Security Server) or press the Enter key to accept the default value if one is specified.

   Example response

   ```
   Enter SAML Request Timeout (default:  10):
   ```

g. When prompted, enter the SAML request timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

   Example response with default values

   ```
   ** Confirm Settings **
   Security Server IP: 45.12.23.56
   Security Server Domain Name:  test3iems.us.nortel.co
   m
   Shared Secret:  nortelnetworks
   Radius Client Timeout:  12
   SAML Connection Timeout:  20
   SAML Request Timeout:  10
   Enter "ok" to commit changes
   Enter "quit" to exit
   Enter anything else to re-enter settings
   ```

h. Accept the PAM configuration update by typing

   ok

   and pressing the Enter key.

   Example response

   ```
   Configuring pam_radius
   configuring nsssaml
   Updating PAM Configuration to use IEMS Security
   Server
   Restarting name service daemon
   ==="pam_radius" completed successfully
   ```

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 To configure a saml password, from the menu prompt in step 3b above:

a. enter the number next to the "saml_passwd_conf (Configure saml password)" option

b. when prompted, enter the default SAML password (slisamadmin) or a new password you have chosen:

Example response

```
** Confirm Settings **
SAML Password:  slisamadmin
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok
Configure Password Successful
=== "saml_passwd_conf" completed
successfully
```

5 If necessary, add the SPFS platform to the IEMS topology. For an SPFS platform user account to be authorized, the SPFS platform must be a RADIUS client of the central security server. For details, see "Adding a Server Platform Foundation Software (SPFS) platform" in IEMS Configuration, NN10330-511.

If a centrally managed restricted access user account is created through the IEMS security application, then the home directory and profile are automatically created. In this case, you do not need to manually configure the user account for platform access.

You have completed this procedure.

—End—

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 (IEMS) central security server. The following third-party Pluggable Authentication Modules (PAMs) are supported:

- "Lightweight Directory Access Protocol (LDAP) PAM" (page 138)

Prerequisites

To perform this procedure, you need to have the root user ID and password for the IEMS central security server, and the LDAP prerequisites below.

LDAP prerequisites

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

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

To configure IEMS Server as an LDAP Client, LDAP PAM and Nsswitch modules must be activated on the server.

Action

Perform the following steps to complete this procedure.

Lightweight Directory Access Protocol (LDAP) PAM

Step Action

At the LDAP server

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

For details on user groups, refer to procedure , if required.

To configure LDAP Security, an LDAP server must be configured with support for Solaris Native LDAP schema and Proxy Authentication. Consult your LDAP server manual for instructions to configure the LDAP server to support Solaris Native LDAP schema.

a. Log in to the LDAP server.

b. Add the necessary user groups to the LDAP server. Consult the LDAP server instructions to add the 25 Succession 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
   - secadm:1026, secrw: 1027, secprov: 1028, secmtc: 1029 secro: 1030

   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
```

   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. Consult your LDAP server instructions to add users to the LDAP server and associte them to usergroups.

   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
```

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

At your workstation

2 Log in to the IEMS server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

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

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Save a backup copy of the nsswitch.conf file, which is located in the */etc* directory.

7

ATTENTION

The **ldapclient** command reconfigures the nsswitch.conf file. It is strongly recommended that you make a backup of nsswitch.conf before executing the **ldapclient** command, and then restore the backup nsswitch.conf file after the **ldapclient** command completes.

Configure the Solaris Native LDAP client and set up proxy authentication on the client using the **ldapclient** command.

Information on the **ldapclient** command, is available at the following link:

http://docs.sun.com/app/docs/db?q=ldap+configuration+guide&p=doc%2F806-5580

8 Replace the nsswitch.conf file with the backup copy of the nsswitch.conf file.

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

a. Add ‘ldap’ as the first option for the password and group.

The entries will look similar to ‘passwd: ldap files’ and ’group: ldap files’ after the change.

This enables the group information to come from LDAP.

10 Restart the name service daemon as follows:

a. # /etc/init.d/nsed stop

b. # /etc/init.d/nsed start

11 Edit the /etc/pam.conf file to include LDAP entries as follows:

a. Add pam_ldap with sufficient setting as the first entry for ‘other auth’, ‘sesm auth’, and ‘secclient auth’ iems entries in the ‘/etc/pam.conf’ file as indicated:

- 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 for ‘other account’, ‘sesm account’, and ‘secclient account’ iems entries in the ‘/etc/pam.conf’ file as indicated:

- 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 for ‘other session’, ‘sesm session’, and ‘secclient session’ iems entries in the ‘/etc/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’

You have completed this procedure.

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 files <userid>`**."

—End—

Reverting the client server to its previous configuration

Application

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

Prerequisites

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

Action

Perform the following steps to complete this procedure.

Step Action

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 SPFS-based server on which you want to revert the configuration

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- OAMP Application Configuration
  4- CORBA Configuration
  5- IP Configuration
  6- DNS Configuration
  7- Syslog Configuration
  8- Remote Backup Configuration
  9- Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19- snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup 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 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
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)
 3 - saml_passwd_conf (Configure saml      password)
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, reprovision the user accounts on the active server. If required, refer to procedure Setting up local user accounts on an SSPFS-based server.

You have completed this procedure.

—End—

Configuring the security server SunOne component to use a new HTTPS certificate

Application

Use this procedure to make the SunOne component use the new server certificate to run in secure mode on the central security server and central security clients.

The activation of SunOne SSL mode is now automatic (part of install/upgrade).

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

- "Simplex configuration (one server)" (page 147)
- "High-availability configuration (two servers)" (page 149)

Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (IEMS) server. If required, refer to procedure "Installing or replacing an HTTPS certificate on an SPFS-based server" (page 151) to install the Apache server's certificate.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

Step Action

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 IEMS 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 by typing

```
# /opt/nortel/applications/security/current_s1isext/sw
mgmt/bin/configure_s1isext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.

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. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

High-availability configuration (two servers)

Step Action

At your workstation

1 Log in 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 IEMS 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 by typing

```
# /opt/nortel/applications/security/current_s1isext/sw
mgmt/bin/configure_s1isext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.

6 Initiate a failover by typing

```
# swact /Y
```

and pressing the Enter key.

7 Reconfigure the SunOne IS client environment on the newly Active server to use SSL by typing

```
# /opt/nortel/applications/security/current_s1isext/sw
mgmt/bin/configure_s1isext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.

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. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Installing or replacing an HTTPS certificate on an HA SPFS-based server

Application

Use this procedure to install or replace an HTTPS certificate on an HA (high availability) SPFS-based server. An HTTPS certificate enables secure transmission of communications, and is required from (I)SN07 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" (page 151)).

Types of certificates

You can use any one of the following three types of security certificates:

- 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 web sites
- 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.

  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.

The certificates differ in the level of trust that needs to be assigned to a server.

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 .
- 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.

  The common name portion of the certificate must match the fully qualified domain name (FQDN) of the server. Nortel recommends the installation of a unique certificate for each host. A separate file contains the key, and must 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

High-availability configuration (two servers)

Step Action

At your workstation

1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure Logging in to an SPFS-based server.

2 Use the following table to determine your next step

If you are	Do
using a self-signed certificate	step 3
otherwise	step 4

3 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/SPFSlog 1024 > server.key
```

and pressing the Enter key.

Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

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.

Enter the command on one line with a space between the -key and server.key entries.

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 Distinguished 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.
------
```

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

   Example response:

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

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

   Example response:

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

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

   Example response:

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

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

   Example response:

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

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

   Example response:

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

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

   Example response:

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

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

Example response:

```
Email Address []:
```

4 Place the certificate file (server.crt) you obtained in ‘/opt/apache/conf/ssl.crt’.

If directory ‘ssl.crt’ does not exist, you need to create it.

5 Place the key file (server.key) in ‘/opt/apache/conf/ssl.key’.

If directory ‘ssl.key’ does not exist, you need to create it.

6 Change the certificate’s owner and group by typing

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

and pressing the Enter key.

Enter the command on one line with a space between "other" and the directory path.

7 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.

Enter the command on one line with a space between "other" and the directory path.

8 Set the certificate permissions by typing

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

and pressing the Enter key.

9 Set the key file permissions by typing

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

and pressing the Enter key.

10 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.

11 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.

12 Use the following table to determine your next step

If	Do
The server is hosting the IEMS	step 14
otherwise	step 22

13 Stop the IEMS server application by typing

```
# servstop IEMS
```

and pressing the Enter key

14 Disable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Disable
```

and pressing the Enter key.

15 Enable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Enable
```

and pressing the Enter key.

16 Start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.

17 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
# /opt/nortel/applications/security/current_s1isext/swm
ext/swmgmt/bin/configure_s1isext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.

18 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.

19 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.

20 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.

21 If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to the procedure "Configuring the SESM server application" in *ATM/IP Configuration Management*, NN10409-500..

22 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.

23 If you installed an HTTPS certificate on an existing SPFS-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

24 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Setting up local user accounts on an SPFS-Based Server

Application

Use this procedure to add local user accounts on a Server Platform Foundation Software (SPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see "Additional information" (page 160).

If you choose to centrally manage your user accounts, refer to procedure "Adding new users" in *IEMS Security and Administration* (NN10336-611).

If you want to launch the ping and traceroute operations that are performed remotely on SPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures "Running a ping test on the GWC network element or SPFS platform" and "Running a traceroute test on the GWC network element or SPFS platform" in *IEMS Basics* (NN10329-111).

ATTENTION
User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

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.

ATTENTION
In a two-server configuration, perform the steps that follow on the active server.

Step Action

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 SSFPS-based server

In a two-server configuration, log in to the active server using its physical IP address.

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 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 -d /export/home/<userid> -g succssn -G
<any additional groups> -m <userid>
```

and press 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 -r files <userid>
```

and press 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.

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" (page 160)) and any other user groups you noted in step 12 to which the user already belonged Include a 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
```

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

You have completed this procedure.

—End—

Additional information

Users of the Nortel 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 following table, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm	secadm
trkrw	lnrw	mgcrw	mgrw	emsrw	secrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov	secmtc
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc	secro
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 following table:

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 OAM&P client applications. The user group operations are listed in the following table:

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.
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov 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.
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" (page 162)
- "Audit operations" (page 164)
- "Carrier provisioning operations" (page 165)
- "Alarm operations" (page 165)
- "Internet transparency operations" (page 165)
- "Trunk provisioning operations" (page 166)
- "Trunk maintenance operations" (page 166)
- "ADSL provisioning operations" (page 167)
- "Line provisioning operations" (page 168)
- "Line maintenance operations" (page 169)
- "V5.2 provisioning operations" (page 169)
- "Patching operations" (page 171)
- "Automated upgrade operations" (page 172)
- "Ping and traceroute operations" (page 172)

The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SPFS-based server.

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

Command	User group				
	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 age nt identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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			
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

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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

Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x
addMPGroup	x	x			
changeMPGroup	x	x			
queryMPGroup	x	x	x	x	x
deleteMPGroup	x	x			
addVPN	x	x			
deleteVPN	x	x			
queryVPN	x	x	x	x	x

Trunk provisioning operations

	User group				
Command	**trkadm**	**trkrw**	**trkmtc**	**trksprov**	**trkro**
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

	User group				
Command	**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 Auto Refresh					x

ADSL provisioning operations

	User group				
Command	**lnadm**	**lnrw**	**lnmtc**	**lnsprov**	**lnro**
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscribe r				x	
Modify cross connection				x	

	User group				
Command	Inadm	Inrw	Inmtc	Insprov	Inro
Delete subscribe r				x	
Delete cross connection				x	

Line provisioning operations

	User group				
Command	Inadm	Inrw	Inmtc	Insprov	Inro
ECHO, QX75, QBB, QBERT, QCM, QCOUNT S, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCO NN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLO AD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	Inadm	Inrw	Inmtc	Insprov	Inro
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
run all TL1 line test commands			x		

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	Inadm	Inrw	Inmtc	Insprov	Inro
Add, delete, modify V5.2 interface		x					x			

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5 Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5 Ring)					x					x
Add, modify, delete ringing cadence mapping (V5 Ring)		x					x			

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View signalling characteristic profile, update list (V5 Sig)					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, auditd, restart, and	x				

	User group				
Command	emsadm	emsrw	emsmtc	emssprov	emsro
smartimage from the NPM GUI or CLUI					
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

	User group									
Command	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Ping and traceroute operations

	User group		
Command	emsadm	emsrw	emsmtc

Launch remote ping	x	x	x
Launch remot e traceroute	x	x	x
These operations are for remote operations performed on SPFS platforms but launched from a centralized GUI on IEMS.			

- "Node provisioning operations" (page 173)
- "Audit operations" (page 175)
- "Carrier provisioning operations" (page 176)
- "Alarm operations" (page 176)
- "Internet transparency operations" (page 176)
- "Trunk provisioning operations" (page 177)
- "Trunk maintenance operations" (page 177)
- "Patching operations" (page 178)
- "Automated upgrade operations" (page 178)

Node provisioning operations

Command	**User group**				
	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
Query a GWC					x
Query an MG					x

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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 age nt identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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 provisio ning		x			
Perform a swact (refer to the notes that follow this table)			x		
Firmware flash			x		
Assign/unassig n services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x

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

Carrier provisioning operations

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

Alarm operations

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

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		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

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

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 15000 Manager GUI		x			

Automated upgrade operations

Command	User group									
	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Deleting local user accounts from an SPFS-based server

Application

Use this procedure to delete local user accounts from a Server Platform Foundation Software (SPFS)-based server.

If you are centrally managing your user accounts, refer to procedure "Deleting users" in the *IEMS Security and Administration* document, (NN10336-611).

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step Action

At your workstation

1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, log in to the active server using its physical IP address.

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.

> **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, nortel

5 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

`userid` is a variable for the user name

You have completed this procedure.

—End—

Configuring DCE on an SPFS-based server

Application

Use this procedure to configure the Distributed Computing Environment (DCE) on a Server Platform Foundation Software (SPFS)-based server following an SPFS 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 SPFS - refer to procedure Unconfiguring DCE on an SPFS-based server in this document, if required
- obtain the following information
  - — the DCE cell name for your customer-provided DCE cell

    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.

Step Action

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 SPFS-based 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 -
```

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 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup 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                         : <value>
DCE Cell Name                     : <value>
Time Server Name                  : <value>
Master Security Server Host Name :  <value>
Master Security Server IP Address:  <value>
CDS Server Host Name              : <value>
CDS Server IP Address:           : <value>
Continue with configuration?(default:Y[Y/N]
```

13 Continue the configuration by typing

y

and pressing the Enter key.

Example response

```
Synchronizing time with <host>......
Tue Apr 16 15:00:47 2002
done synchronizing time with <host>(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, <host>, 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:  <host>
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, <host>, was successful.
Configuration completed successfully.
done configuring DCE
Gathering current configuration information...
Configuration of DCE Host, <host>, will now begin.
There are no components in the request that need to be
configured.
Gathering component state information...
Component Summary for Host:  <host>
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, <host>, was successful.
Configuration completed successfully.
=== "dce_conf" completed successfully
```

15 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

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.

Step Action

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 SPFS-based server on which you want to configure the SSO token

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 - Remote Backup Configuration
 10 - Database Configuration
 11 - NFS Configuration
 12 - Bootp Configuration
 13 - Restricted Shell Configuration
 14 - Security Services Configuration
 15 - Disk Drive Upgrade
 16 - Login Session
 17 - Location Configuration
 18 - Cluster Configuration
 19 - Succession Element Configuration
 20- snmp_poller (SNMP Poller Configuration)
 21 - backup_config (Backup 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.

You have completed this procedure.

—End—

Security Token Administration GUI overview

IEMS Security Token Administration GUI can be used to:

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

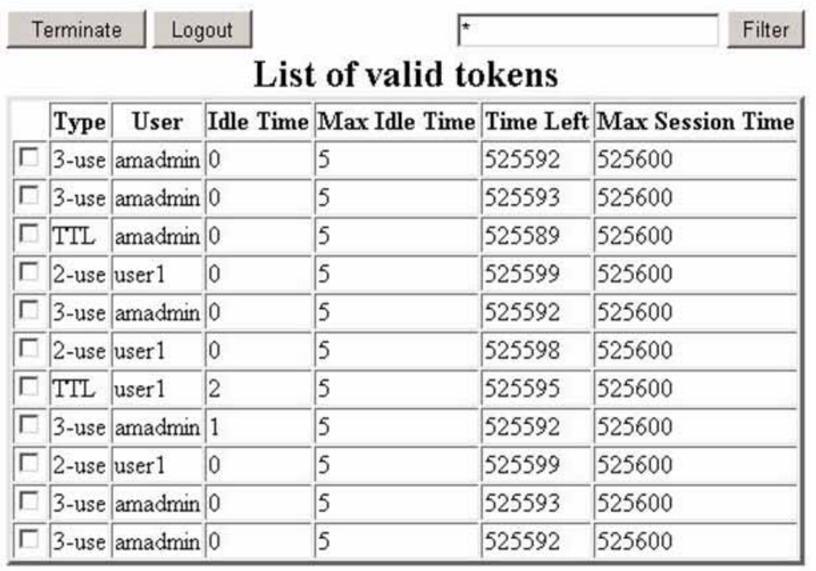
IEMS Security Token Administration GUI displays all of the user sessions that are available to the Identity Server and displays the expiration time for each session. See "List of valid tokens window" (page 191).

IEMS 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 IEMS Security Token Administration GUI, see "Launching the IEMS Security Token Administration GUI" (page 192).

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 IEMS Security Token Administration GUI

Application

Use this procedure to launch the IEMS Security Token Administration GUI.

Prerequisites

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

To verify that the user account is set up, see the procedure for "Listing all groups and users" (page 22).

Action

Step	Action

At a web browser

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

```
https://hostname:8443/tokenadmin
```

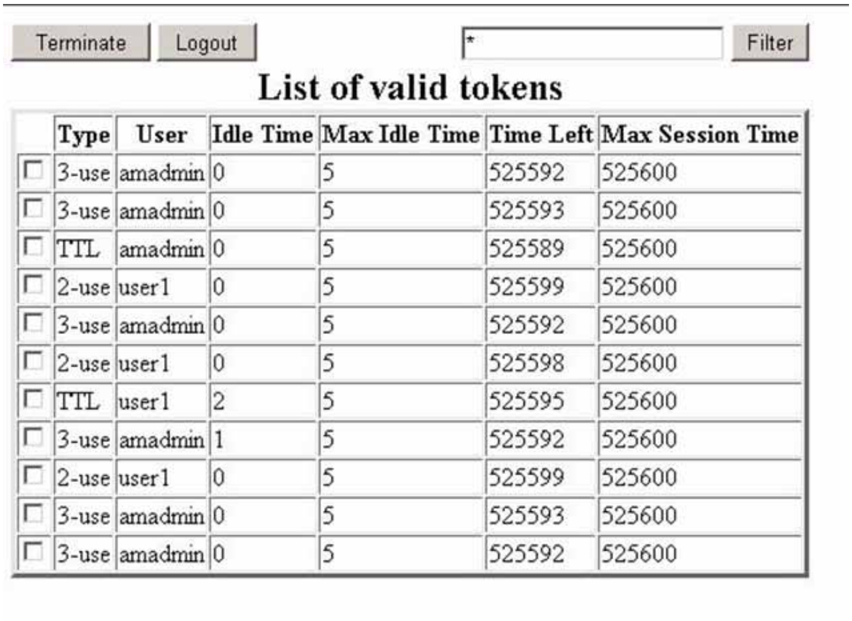
The Token Management window is displayed.

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 as follows:



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

5 You have completed this procedure.

—End—

Viewing a user session

Application

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

Step Action

At the IEMS Security Token Administration GUI

1 Log in to the IEMS Security Token Admininstration GUI.

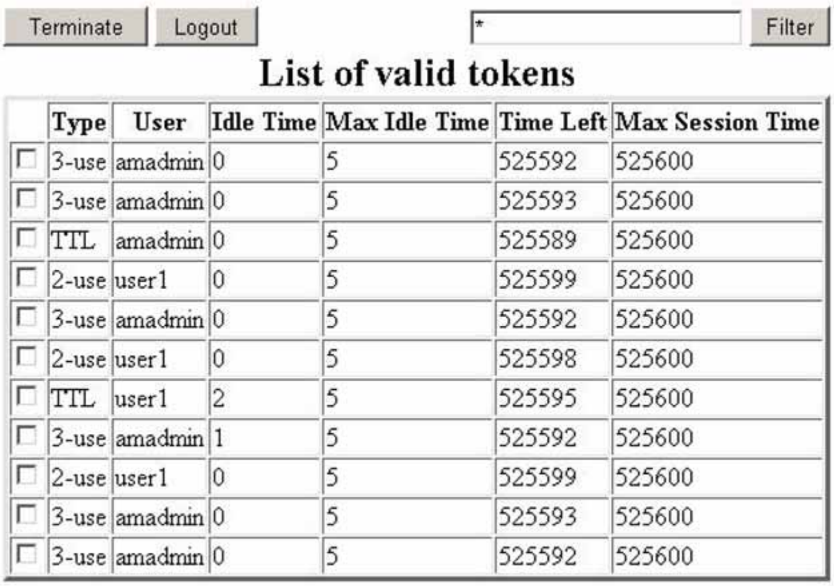
a. Open the Token Management window. See "Launching the IEMS Security Token Administration GUI" (page 192).

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.

4 You have completed this procedure.

—End—

Terminating a user session

Application

Use this procedure to terminate a user session.

Prerequisites

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

Action

Step **Action**

At the IEMS Security Token Administration GUI

1 Log in to the IEMS Security Token Admininstration GUI.

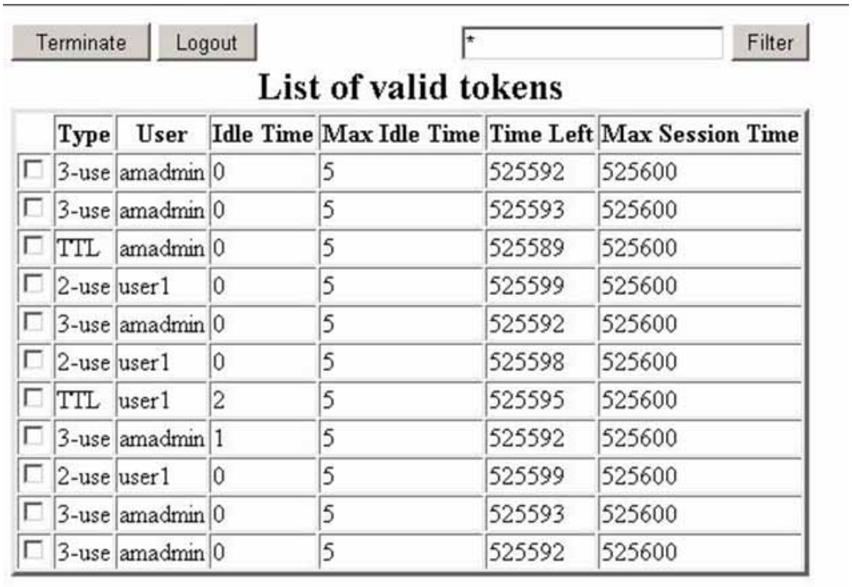
a. Open the Token Management dialog box. See "Launching the IEMS Security Token Administration GUI" (page 192).

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**.

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

4 You have completed this procedure.

—End—

Health Monitors overview

If the Central Security Server's framework components fail, no security clients can access security services provided by the IEMS Central Security Server. Smart health monitors are provided to ensure the crucial security components are not dead or hung. In such situations, the failed components will be automatically restarted. There are three health monitors included on the IEMS server:

- Sun Identity Server health monitor
- Radius Server health monitor
- PAM login servlet health monitor

The health monitors are automatically started by the system after the monitored process starts and are disabled when the monitored process is stopped.

Sun Identity Server health monitor

The identity server health monitor checks the health of the Sun Identity Server with the following three tests:

- Attempts to login with the user ’unknown’. This user should not be in the system and the login should fail with the proper return values from the server to indicate the server is still functioning.
- Performs a policy check with a system user. The policy test should succeed and indicate that the system user was able to login and perform the policy check.
- Confirms that the nsswitch configuration of the server works and the group ’secadm’ can be retrieved through a query to nsswitch.

When any test fails, a customer log, EMSS 314, is generated and the health monitor restarts the Identity Server process group automatically. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

Radius Server health monitor

The Radius Server attempts to log in through the Radius Server using an invalid user name and password. The Radius Server should reply to a client with a message to indicate that the login failed. When the test fails, a customer log, EMSS 313, is generated. The Radius Server health monitor restarts the RADSVR process group automatically. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

PAM Login Servlet health monitor

The PAM login servlet health monitor attempts to retrieve the following URL:

https://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown

If this fails, the health monitor attempts to retrieve the following URL, which does not use SSL:

http://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown

After verifying that the WEBSERVICES process group is running, a customer log, EMSS 315, is generated to indicate the PAM login servlet was unhealthy and that WEBSERVICES is being restarted. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

Backup and restore

Backup and restore on IEMS

As IEMS resides on the SPFS platform, it executes the backup and restore policy defined for the SPFS platform. For more details on the backup and restore procedures, refer to *ATM/IP Solution-level Administration and Security*, NN10402-600.

Use the procedures in this section to do the following:

- Backup the central security server
- Backup and SPFS-based security client
- Restore the central security server
- Restore Core Element Manager data

Synchronous backup manager (SBRM)

You can use the Synchronous backup restore manager (SBRM) to backup the SPFS data, including the security client data and oracle data. See Synchronized Backup Manager overview in *ATM/IP Solution-level Administration and Security*, NN10402-600 for details.

Automated backup and restore tool

The Automatic Backup and Accelerated restore feature, referred to as ’remote backup’ is specific to geographically-dispersed configurations.

The Automatic Backup and Accelerated restore feature, referred to as ’remote backup’ will remotely backup all data on the ’target’ unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (for example, catastrophic site loss).

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup which can be scheduled to automatically occur from once a day to four times per day. This tool also provides a facility for manually initiating a backup and monitoring its progress. The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

For details about geographic survivability and remote backup, refer to *Carrier VoIP Solutions Disaster Recovery Procedures*, NN10450-900.

Backing up the central security server

Application

Use this procedure to back up the central security server. When the Security Services component is installed, the generic backup and restore script (brr_security.sh) are registered with servman (bkmgr).

The NDS database and all files under the following directories are backed up using this procedure:

- /opt/nortel/config/3rd_party/netscape
- /opt/nortel/config/3rd_party/security/s1is
- /opt/nortel/config/applications/security
- /opt/nortel/data/3rd_party/netscape
- /opt/nortel/data/3rd_party/security/s1is
- /opt/nortel/data/applications/security

Prerequisites

You must have root user privileges to perform this procedure.

Action

Step Action

At your workstation

1 Establish a connection to the server where IEMS resides through telnet or SSH, using the host name or IP address of the server, and log in using the root user ID and password.

In a two-server configuration, establish the connection to the active server using the physical IP address of the active server, and ensure you are on the active server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server.

2 Use the following table to determine your next step.

If	Do
this server is hosting the CMT and IEMS	step 3
this server is only hosting the IEMS	step 6

3 Verify the status of the SESM server application by typing

```
servman query -status -group SESMService
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If	Do
the SESM server application is running	step 6
otherwise	step 5

5 Start the SESM server application by typing

```
servstart SESMService
```

and pressing the Enter key.

6 Enter the backup manager utility by typing

```
/opt/bkresmgr/cbm/bkmgr
```

and pressing the Enter key.

7 Start the backup by typing

```
backup full
```

and pressing the Enter key.

8 Use the following table to determine your next step.

If response is	Do
Backup succeeded.	step 9
Backup failed. For more detailed errors, refer to log file at ...	Contact your next level of support.

9 Exit the backup manager utility by typing

```
quit
```

and pressing the Enter key.

The Security Services configuration settings and data are backed up to the following file:

/data/bkresmgr/<date><time>backupSS1.1<host_name>.tar

10 You have completed this procedure.

If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Backing up an SPFS-based security client

Application

Use this procedure to obtain a list of the files that will be backed up from the client machine. To enable backup and restore of the security client, the files to be backed up are registered with servman during installation. The files backed up depend on the packages installed.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Step Action

In a telnet connection to the security server

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 server where IEMS 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 Enter the following command:

```
cat etc/critdata.conf
```

The system returns a list of all non-oracle data files that will be backed up from the client machine.

6 Use the Synchronous Backup Restore Manager (SBRM) to backup the central security client data. When SBRM is run, all of the SPFS data, including the security client data and oracle data, is backed up. For details, see the procedure for "Starting or stopping the automated synchronous backup restore manager service" in *ATM/IP Solution-level Administration and Security*, NN10402-600.

7 You have completed this procedure.

—End—

Restoring the central security server

Application

Use this procedure to restore the security server from a backup file.

> **ATTENTION**
>
> SSL uses certificates. Certificates from one server cannot be used on another server. If you want to take a back up file from a server where SSL is implemented and restore to a different server, you must perform the procedure "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed. This script is run to set up IS authentication, session, and policy traffic to operate under SSL.
>
> Note that servers in the same high availability cluster can use the same SSL certificate.
>
> Note that if the restored IS SSL certificate has expired, you must perform the procedure in "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed.

Prerequisites

This procedure has the following prerequisites:

- You must have root user privileges.
- You must have a backup tar file created using the procedure for "Backing up the central security server" (page 203).

Action

Perform the following steps to restore central security server data.

Step Action

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 server

If you are upgrading the active server, telnet to the active server. If you are upgrading the inactive server, telnet to the inactive 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.

If	Do
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step 7
otherwise	step 5

5 Stop the security services by doing the following:

a. Type:

```
servstop RADSVR
```

and press the Enter key.

b. Type:

```
servstop IS
```

and press the Enter key.

c. Type:

```
servstop WEBSERVICES
```

and press the Enter key.

6 List the available security server backup files and determine the backup file to be restored by typing:

```
ls /data/bkresmgr
```

and pressing the Enter key.

The format of the security server backup files are **<data><time>backupSS1.1<host_name>.tar**

Note the name of the security server backup file you intend to restore. You will need this information in a later step.

7 Change directories by typing:

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

and pressing the Enter key.

8 Determine if SAML is enabled on the workstation by looking at the nsswitch.conf file.

Type:

```
vi /etc/nsswitch.conf
```

press the enter key
if: the following is seen:

```
passwd:     files
group:      files
```

do: continue to step 10

if: saml is seen in the two lines, for example:

```
passwd:     saml  files
group:      saml  files
```

do: continue to step 9

9 Disable SAML by typing:

```
vi /etc/nsswitch.conf
```

press the enter key
replace the "passwd:" & "group:" lines with the following:

```
passwd:     files
group:      files
```

save and close the file

10 Perform the restore operation by typing:

```
./brr_security.sh -restore /data/bkresmgr/<date><time>backupSS1.1<host_name>.tar
```

where <date><time>backupSS1.1<host_name>.tar is the backup file from which you are restoring.

Press the Enter key.

If	Do
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step 13
otherwise	step 11

11 Restart the security services by doing the following:

a. Type:

```
servstart WEBSERVICES
```

and press the Enter key.

b. Type:

```
servstart IS
```

and press the Enter key.

c. Type:

```
servstart RADSVR
```

and press the Enter key.

12 Enable SAML by typing:

```
vi /etc/nsswitch.conf
```

and press the Enter key.

replace the passwd: & group: lines with the following:

```
passwd:     saml files
group:      saml files
```

save and close the file.

13 If the restored image was backed up from a different server with a different certificate or if the restored certificate has expired, follow the procedure in "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 to replace the invalid or expired certificate on the IEMS Server.

14 Select your next step.

If you are restoring a server	Do
in a simplex configuration	step 17
in a high-availability configuration	step 15

15 Select your next step.

If	Do
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step 17
otherwise	step 16

16 Clone the active server to the inactive server. For details, see "Cloning the image of one node in a cluster to the other node" in *ATM/IP Solution-level Administration and Security*, NN10402-600.

17 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Restoring Core Element Manager data

Application

Use this procedure to restore Core Element Manager (CEM) data.

The backup procedure is performed through the Synchronous backup restore manager (SBRM). See Synchronized Backup Manager overview in *ATM/IP Solution-level Administration and Security*, NN10402-600 for details. The information needed by the Core Element Manager to restore data is located in /opt/nortel/cem/data/coreEMS/configBackup.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Step Action

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 server where the CEM resides

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 Make sure that the /opt/nortel/cem/data/coreEMS/configBackup directory contains the following files:

- data_dir
- ldapConfig.tar
- nodes.tar
- server

Enter:

```
# ls /opt/nortel/data/coreEMS/configBackup
```

6 Make sure that CEM is not running by typing:

```
# servquery -status -group CEM
```

and pressing the Enter key.

Example response:

CEM server STOPPED

7 If the CEM server is running, stop the CEM server by typing:

```
# servstop CEM
```

and pressing the Enter key.

Example response:

CEM server successfully stopped

8 Run the restore script by typing

```
#/opt/nortel/cem/data/coreEMS/nodes/server/bin/postRe
store.sh
```

and pressing the Enter key.

9 You have completed this procedure.

—End—

Logging in to an SPFS-based server

Application

Use this procedure to log into a Server Platform Foundation Software (SPFS) server. This procedures provides the steps to establish a login session using SSH, which is secure, or telnet, which is not secure.

Some tasks will require that you log in to the server through the console (port A) using the root user ID and password.

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server

  In a two-server configuration, you need the physical IP address of the active or inactive server.
- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

Perform the steps under one of the following headings to complete this procedure.

- Logging in using SSH
- Logging in using Telnet
- Logging in through the console

Logging in using SSH

Step Action

At your workstation

1 Establish an SSH session.

If you have access to a workstation which supports the ssh command (Linux, for example) then proceed with step a.

Otherwise, connect to the server using an SSH client and proceed to step 2.

a. Establish an SSH session to the server by typing

```
> ssh -l <user_id> <server>
```

where

user_id is root or your user id
server is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

2 Use the following table to determine your next step.

If you receive	Do
a message indicating a host authentication issue and a request to continue the connection	step 3
a prompt for a password	step 4

> **ATTENTION**
> The prompt indicates SSH is verifying whether the server is a trusted host for the workstation. SSH performs the verification the first time SSH is run on a workstation.

3 Continue the connection by typing

```
y
```

and pressing the Enter key.

4 Enter the password for root or your user id and press the Enter key.

5 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 9
two-server configuration	step 6

6 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

7 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8

If you need to be on the	Do
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

8 You are logged in to the wrong server. Return to step 1 to log in to the other server.

9 You have completed this procedure.

If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in using Telnet

Step Action

At your workstation

1 Establish a telnet session to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or hostname of the SPFS-based server, or the physical IP address of the active or inactive server in a two-server configuration

2 When prompted, enter your userid.

ATTENTION

You cannot log in using the root userid at this step.

3 When prompted, enter your password.

4 Use the following table to determine your next step.

If	Do
you need to log in as root	step 5
otherwise	step 7

5 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 11
two-server configuration	step 8

8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

9 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 10
inactive server and the response is ClusterIndicatorACT	step 10
active server and the response is ClusterIndicatorACT	step 11
inactive server and the response is ClusterIndicatorSTBY	step 11

10 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

11 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in through the console

Step Action

At the console connected to the server

1 Log in to the server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the active or inactive server as required.

2 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 6
two-server configuration	step 3

3 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 5
inactive server and the response is ClusterIndicatorACT	step 5
active server and the response is ClusterIndicatorACT	step 6
inactive server and the response is ClusterIndicatorSTBY	step 6

5 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

6 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Configuring X.509 digital certificates using Certificate Manager

Digital certificates are used to support IPSec to ensure secure call control message communications. They can also be used for secure communication between element managers and network elements.

The IEMS server hosts the centralized Certification Authority or trust center responsible for the management of private keys and digital certificates used in IPSec/IKE authentication.

Certificate Manager provides the ability to automate the tracking and management of certificate replacement for the following supported devices. These devices are also known as integrated devices:

- MG 9000 Manager
- MG 9000
- GWC Manager
- GWC
- SSM
- SPFS
- WebServices

Use the following procedures to configure digital certificates using Certificate Manager.

- Launching the Certificate Manager in *IEMS Overview*, NN10329-111
- Adding a Certificate Manager application in *IEMS Configuration*, NN10330-511
- Adding a Certificate Manager application using Web Client in *IEMS Configuration*, NN10330-511
- "Configuring the entity default values for Certificate Manager" (page 223)
- "Configuring the broker default values for Certificate Manager" (page 228)

Configuring the entity default values for Certificate Manager

Application

Use this procedure to modify the default Distinguished Subject Name (or Entity Default) of the Root Certificate Authority (CA). The root CA is also known as the Trust Anchor. The name components are used to create the subject identity field of certificates generated by the Certificate Manager CA and modifying these names results in the replacement of all certificates including the Certificate Manager CA certificates.

Use this procedure on initial configuration of the Certificate Manager only.

ATTENTION

Possible service outage

You must perform this procedure during the initial configuration of Certificate Manager before generating or importing any X.509 certificates. Performing this procedure after generating or importing an X.509 certificate may cause a service outage.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.
- you must be a member of the emsadm group.
- the entire office update must be complete

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview* NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview* NN10453-100.

2 Check whether there are any existing certificates. If any certificates already exist, modifying the entity defaults can cause a service outage. To do so, perform the following steps:

a. Click the **Browse** link.

The Browse Operations window opens.

b. Click the **View Certificates** link.

The Certificate Types window opens.

c. Select all entity types from the drop-down list. Hold down the Ctrl key to select more than one entity type.

3 Click the **certListing** button.

A table of certificate summary information is displayed.

4 Select your next step.

If	Do
any certificates are listed	do not continue this procedure. Exit this procedure and contact your next level of support.
no certificates are listed	go to the next step. **CAUTION** Exiting this procedure after clicking the OK button in the confirmation dialog box which directs you to the CA certificate replacement window will cause a service outage.

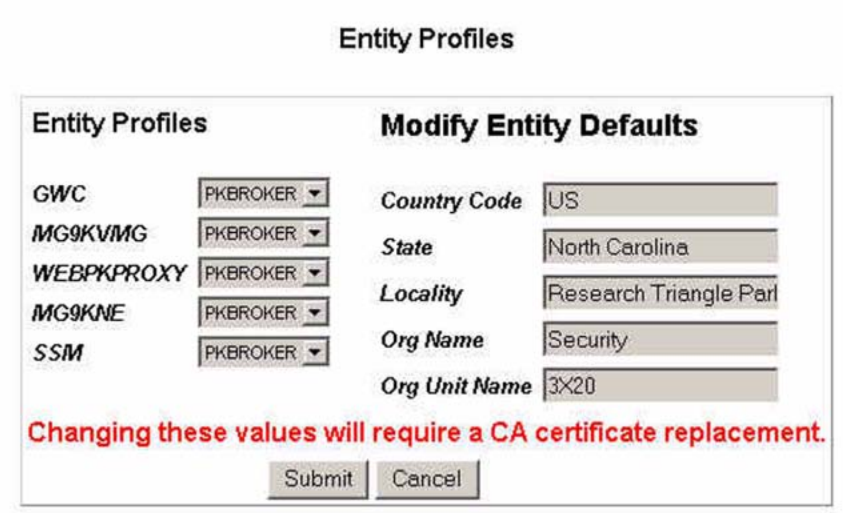
5 Click the **Home** link to return to the home page.

6 Click the **Configure Broker** link.

The Configure Defaults window opens.

7 Click the **Entity Settings** link.

The Entity Profiles window opens. The window lists the integrated devices and the name components that are used to create the subject identity field of certificates



Entity Profiles

Entity Profiles

GWC	PKBROKER
MG9KVMG	PKBROKER
WEBPKPROXY	PKBROKER
MG9KNE	PKBROKER
SSM	PKBROKER

Modify Entity Defaults

Country Code	US
State	North Carolina
Locality	Research Triangle Parl
Org Name	Security
Org Unit Name	3X20

Changing these values will require a CA certificate replacement.

The descriptions of the fields are listed in the following table.

Field	Description
Entity Profiles	Lists each of the entity types integrated with the Certificate Manager
Entity Profiles drop-down list	Displays the certificate authority that is the source for the certificates of each entity
Modify Entity Defaults	
Country	An identifier which defines the country code according to ISO standard ISO 3166. The identifier has two characters, is case-insensitive and is limited to alphabetic characters (a - z).
State	An identifier which defines an area such as the state or province. The identifier has a 30 character limit and can consist of alphanumeric characters (a-z, A-Z, 0-9).
Locality	An identifier which defines the locality. The identifier has a 30 character limit and can consist of alphanumeric characters (a-z, A-Z, 0-9).
Org Name	An identifer which defines the organization name. The identifier has a 30 character limit and can consist of alphanumeric characters (a-z, A-Z, 0-9).
Org Unit Name	An identifier which defines the organization unit name. The identifier has a 30 character limit and can consist of alphanumeric characters (a-z, A-Z, 0-9).

The following special characters are not allowed to be entered into the Modify Entity Defaults fields (Country, State, Locality, Org Name, Org Unit Name):

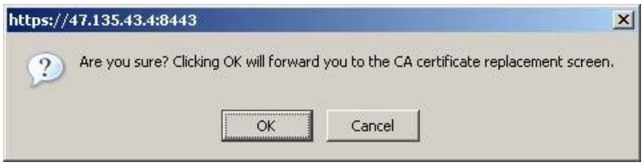
~ ‘ ! @ # $ % ^ & * ( ) _ - + = { [}] | \ : ; " ’ < , > . ? /

8 To update the entity profile, use PKBROKER as the entity profile for each device type.

9 Click the **Submit** button.

10 Click the **Confirm** button.

A dialog box similar to the following figure opens:



Are you sure? Clicking OK will forward you to the CA certificate replacement screen.

11 Click the **OK** button in the confirmation dialog box to be redirected to the CA certificate replacement window.

> **ATTENTION**
>
> **Possible service outage**
>
> You must click the **OK** button. If you click the **Cancel** button, the data provided is still committed and a root CA replacement is not initiated. If a root CA replacement is not initiated, a service outage may occur.

12 Click the **Submit** button.

The following warning message appears:

"This operation replaces ALL integrated device certificates in the network! Use with extreme caution."

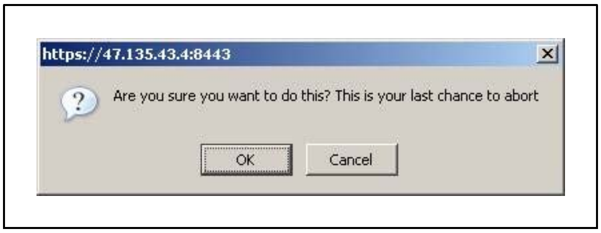
13 Click the **Submit** button in the CA Certificate window.

The following warning message appears:

"This operation replaces ALL integrated device certificates in the network! Use with extreme caution. The potential for an outage exists with this operation! Cancel to abort."

14 Click the **Confirm** button.

A warning dialog box similar to the following graphic opens:



https://47.135.43.4:8443

Are you sure you want to do this? This is your last chance to abort

15 Click the OK button to revoke the CA certificate.

A message appears that reads

CA Certificate Replacement in Progress. Read-Only Operations Allowed."

16 Click the **Submit** button in the CA Certificate window.

17 After five minutes, click the **Home** menu item.

The message, "CA CertificateReplacement in Progress. Read-Only Operations Allowed." no longer appears.

The Certificate Manager is now ready for certificate generation and certificate import.

18 You have completed this procedure.

—End—

Configuring the broker default values for Certificate Manager

Application

Use this procedure to set default values for Certificate Manager alarm thresholds for each supported entity type. This procedure should be used during the initial setup of Certificate Manager on SPFS.

Nortel recommends that you use the default values.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview,* NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,* NN10453-100.

2 Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Configure Broker** link.

The Configure Defaults window opens.

4 Click the **Broker Settings** link.

The Modify Broker Defaults window opens.The descriptions of the fields are listed in the following table.

Field	Description
Device	Lists the integrated devices

Field	Description
Minor Alarm	Defines the alarm threshold in hours to generate a minor alarm. The default for all devices (except the GWC) is the minimum recommended value of 168 hours. The default recommended value for the GWC is 840 hours (35 days). The Certificate Manager automatically raises an alarm when device certificates that are expiring within the minor alarm value. In that case, the Certificate Manager attempts to recreate and deliver the respective certificate. If successful, the alarm clears automatically. If the Certificate Manager is not successful, the alarm continues to be raised.
Major Alarm	Defines the alarm threshold in hours to generate a major alarm. The default for all devices (except the GWC) is the minimum recommended value of 72 hours. The default recommended value for the GWC is 420 hours (17.5 days).
Cert. Expiry	Defines the number of days a generated certificate is valid in the system. The certificate expires after this period. The recommended default is 365 days. This value should not be set to lower than 90 days. ***Note:*** The values must follow the rule that Cert. expiry must be at least 24 hours greater than the minor alarm.

5 Modify the broker default fields as required. Nortel recommends that the default values are not changed.

6 Click the **Submit** button.

7 Click the **Confirm** button.

8 Click the **OK** button in the confirmation dialog box.

An Operation successful message appears.

9 You have completed this procedure.

—End—

Viewing certificates using Certificate Manager

Application

Use this procedure to do view a certificate according to its device hierarchy.

Prerequisites

This procedure has the following prerequisites:

- You must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview,* NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,* NN10453-100.

2 Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Browse** link.

The Browse Operations window opens.

4 Click the **View Certificates** link.

The Certificate Types window opens.

5 Select the entity types from the drop-down list that you want to view in the certificate summary.

Hold down the Ctrl key to select more than one entity type.

The certificate types are listed in the following table.

Certificate Type	Description
GWC	GWC uses certificates for call processing control IPSec IKE communication with gateways
MG9KVMG	MG 9000 uses certificates for call processing control IPSec IKE communication with the gateway controller

Certificate Type	Description
MG9KNE	The MG 9000 NE uses certificates for OAM&P IPSec IKE communication with the MG 9000 element manager
WEBPKPROXY	The Apache/Tomcat Certificate Manager proxy uses certificates for HTTPS connections to Web browsers and servlets. WEBPKPROXY certificates must be installed manually. When these certificates are created for the first time, they remain in the CREATED state until the certificate is installed. On subsequent creation attempts, they go to the DELIVERED state when they have been placed in the /data/pkclient/certificates directory on the target device. The certificates must then be installed manually.
SSM	SSM uses certificates for OAM&P IPSec IKE communication used by the MG 9000 element manager to communicate with the MG 9000 network element.
GENERICINTERNAL	Certificates that are created by the Certificate Manager and are for use by devices and entities that are not integrated with the Certificate Manager. The Certificate Manager monitors these certificates for expiration and cannot revoke or replace these certificates automatically. These certificates must be deleted and replaced manually. For (I)SN09U, this certificate type is not supported.
INHERITINTEGRATED	Certificates that are created by a third party infrastructure and are monitored for expiration by the Certificate Manager. For (I)SN09U, this certificate type is not supported.

6 Click the **certListing** button.

A table of certificate summary information is displayed.

7 Click the Common Name link of the item you want to view in detail.

The full details of the certificate are displayed in the Certificate Details window. The details of the certificate are listed in the following table.

Field	Description
Common Name	Displays the name of the certificate.
Serial#	Displays the serial number of the certificate.
Active Date	Displays the date and time when the certificate became active.
Expiry Date	Displays the expiry date and time of the certificate.
Issuer	Displays the name of the certificate authority that issued the certificate.
Type	Displays the source of the certificate. CA indicates that the source is an internal certificate authority.
Manager ID	Displays the element manager deploying the certificate.
Cert State	Displays the state of the certificate. REPLACE - the Certificate Manager is in the process of replacing the certificate when it is expiring or has been revoked. The Certificate Manager will attempt to contact the element manager for the given device. GENERICINTERNAL certificates will not advance from this state because they are not integrated with the Certificate Manager. To advance to the CREATED or DELIVERED state, you must first delete and then re-create GENERICINTERNAL certificates. CREATED - the Certificate Manager has successfully contacted the element manager for the given device, has created the certificate for a given device, and is attempting to deliver the certificate. DELIVERED - the Certificate Manager has successfully delivered the certificate to the given device. In the case of WEBPKPROXY certificates, ensure that the certificate has been installed to avoid a service outage by verifying that no PKM306 alarms exist in the network.

8 You have completed this procedure.

—End—

Viewing alarms using Certificate Manager

Application

Use this procedure to view the alarm details generated by Certificate Manager.

For details on Carrier VoIP logs and alarms, refer to *Carrier VoIP Fault Management Logs Reference guide*, NN10275-909.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step	Action
At the IEMS workstation	
1	Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,* NN10453-100.
2	Click the **Browse** link. *The Browse Operations window opens.*
3	Click the **View Alarms** link. *A Severity list is displayed.*
4	Select the severity of the alarms that you want to view and click the **alarmListing** button. *A table of active alarm information is displayed.*
5	Click the entry of the alarm you want to view in detail. *The full details of the alarm are displayed in the Alarm Details window.*
6	You have completed this procedure.

—End—

Deleting a GENERICINTERNAL certificate using Certificate Manager

Application

Use this procedure to delete a GENERICINTERNAL certificate when the certificate is no longer required, or has expired and must be recreated. Once unmanaged, a GENERICINTERNAL certificate can be deleted. GENERICINTERNAL certificates are used by devices that are not integrated with the Certificate Manager. The creation, deployment, replacement, and deletion procedures are done manually.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,*NN10453-100.

2 Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Manage Certificates** link.

The Management Operations window opens.

4 Click the **Modify Cert state** link.

The Certificate Listing window opens.
The descriptions of the fields are listed in the following table.

Field	Description
Action	Drop-down list with option to manage or unmanage the certificate
Common Name	Displays the name of the certificate

Field	Description
Type	Defines the type of certificate
Serial#	Displays the serial number of the certificate
Cert State	Displays the state of the certificate. REPLACE - GENERICINTERNAL certificates in the REPLACE state can only be deletedD or DELIVERED state, GENERICINTERNAL ce. The Certificate Manager displays this state if a GENERICINTERNAL certificate was revoked or has expired. GENERICINTERNAL certificates do not advance from this state because they are not integrated with the Certificate Manager. To advance to the CREATErtificates must be first deleted and then re-created. CREATED - GENERICINTERNAL certificates in the CREATED state can be managed or deleted. A GENERICINTERNAL certificate in this state can be deleted. There will be no impact to the device that is using the certificate. However, the Certificate Manager will not be able to monitor the certificate for expiration. DELIVERED - GENERICINTERNAL certificates in the DELIVERED state must be unmanaged before deletion. Once managed, the certificate can be deleted. A GENERICINTERNAL certificate in the DELIVERED state is monitored for expiration.

5 Select the checkbox next to the certificate you want to delete.

6 Select your next step.

If the certificate state is	Do
CREATED or REPLACE	delete the certificate. Proceed to step 10.
DELIVERED	unmanage the certificate before deletion. Proceed to step 7.

7 Select **Unmanage** from the drop-down list.

8 Click the **Submit** button.

9 Click the **Confirm** button.

10 Select **Delete** from the drop-down list under the Action column.

11 Click the **Submit** button.

12 Click the **Confirm** button.

The message *"Operation Successful"* appears.

13 You have completed this procedure.

—End—

Deleting a WEBPKPROXY certificate using Certificate Manager

Application

Use this procedure to delete a WEBPKPROXY certificate that is used by Apache and Tomcat when an element manager is decommissioned or when support activities are performed. Ensure that the element manager is no longer using the certificate before you perform this procedure.

> **ATTENTION**
>
> **Possible service outage**
>
> If an element manager is using the WEBPKPROXY certificate that you delete, this can cause a service outage.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step	Action
At the IEMS workstation	
1	Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,*NN10453-100.
2	Enter your user name and password to log into the Certificate Manager GUI.
3	Click the **Manage Certificates** link. *The Management Operations window opens.*
4	Click the **Modify Cert state** link.

The Certificate Listing window opens. The descriptions of the fields are listed in the following table.

Field	Description
Action	Drop-down list with option to manage or unmanage the certificate
Common Name	Displays the name of the certificate
Type	Defines the type of certificate
Serial#	Displays the serial number of the certificate
Cert State	Displays the state of the certificate. WEBPKPROXY certificates are integrated with the Certificate Manager. REPLACE - WEBPKPROXY certificates in the REPLACE state can be deleted. The Certificate Manager displays this state if a WEBPKPROXY certificate was revoked but the target application on the element manager has not yet responded to requests to replace its certificate. To advance the certificate to the CREATED or DELIVERED state, the target application on the element manager must respond to requests to replace its certificate. CREATED - WEBPKPROXY certificates in the CREATED state can be deleted. A WEBPKPROXY certificate in this state has been created, but has not yet changed to the DELIVERED state. On initial creation, WEBPKPROXY certificates must be installed and registered manually. Once this is complete, the certificate changes to the DELIVERED state. On subsequent replacements, WEBPKPROXY certificates change to the DELIVERED state when they have been placed in the /data/pkclient/certificates/ directory on the element manager. After WEBPKPROXY certificates are placed in the /data/pkclient/certificates/ directory, they must be installed and registered manually for them to take effect. DELIVERED - WEBPKPROXY certificates in the DELIVERED state must be unmanaged before deletion. Once unmanaged, the certificate can be deleted. While a WEBPKPROXY certificate is in the DELIVERED state, the Certificate Manager monitors the certificate for expiration and supports automatic replacement when the certificate expires or is revoked.

5 Select the checkbox next to the certificate you want to delete.

6 Select your next step.

If the certificate state is	Do
CREATED	step 10
DELIVERED	step 7

7 Select **Unmanage** from the drop-down list.

8 Click the **Submit** button.

9 Click the **Confirm**button.

The message "Operation Successful appears".

10 Select **Delete** from the drop-down list under the Action column.

11 Click the **Submit** button.

12 Click the **Confirm**button.

The message "Operation Successful appears".

13 You have completed this procedure.

—End—

Managing a GENERICINTERNAL certificate using Certificate Manager

Application

Use this procedure to manage a GENERICINTERNAL certificate and monitor the certificate for expiration. GENERICINTERNAL certificates are used by devices that are not integrated with Certificate Manager. The creation, deployment, replacement, and deletion procedures are performed manually.

GENERICINTERNAL certificates in the CREATED state can be managed or deleted. When managed is selected, the certificate state is changed to DELIVERED.

GENERICINTERNAL certificates in the DELIVERED state can be unmanaged. When unmanage is selected, the certificate state is changed to CREATED. Once in this state, the certificate can be deleted.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,*NN10453-100.

2 Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Manage Certificates** link.

The Management Operations window opens.

4 Click the **Modify Cert state** link.

The Certificate Listing window opens.

The descriptions of the fields are listed in the following table.

Field	Description
Action	Drop-down list with option to manage or unmanage the certificate
Common Name	Displays the name of the certificate
Type	Defines the type of certificate
Serial#	Displays the serial number of the certificate
Cert State	Displays the state of the certificate. REPLACE - GENERICINTERNAL certificates in the REPLACE state can only be deleted. The Certificate Manager displays this state if a GENERICINTERNAL certificate was revoked. GENERICINTERNAL certificates do not advance from this state because they are not integrated with the Certificate Manager. To advance the certificate to the CREATED or DELIVERED state, GENERICINTERNAL certificates must first be deleted and then re-created. CREATED - GENERICINTERNAL certificates in the CREATED state can be managed and changed to the DELIVERED state. DELIVERED - GENERICINTERNAL certificates in the DELIVERED state are already managed.

5 Select the checkbox next to the certificate you want to manage.

6 Select your next step.

If the certificate state is	Do
CREATED	the next step
DELIVERED	the certificate is already managed. You have completed this procedure.
REPLACE	the certificate cannot be managed. You have completed this procedure.

7 Select **Manage** from the drop-down list under the Action column.

8 Click the **Submit** button.

9 Click the **Confirm** button.

The message "Operation Successful appears".

10 You have completed this procedure.

—End—

Generating and exporting GENERICINTERNAL certificates

Application

Use this procedure to install and use a GENERICINTERNAL certificate and trusted certificates are written to the /data/NTPkmgr/cert/export directory.

This procedure is also used to export or re-export a previously created GENERICINTERNAL type certificate as in the case where a GENERICINTERNAL certificate has been revoked and the export directory is being updated or another copy of a certificate is required.

This procedure generates a private key and public key pair. The public key is certified and placed in the certificate. The private key, certificate, CA chain, and trusted certificate are written to the cert/export directory as a result of this procedure.

GENERICINTERNAL certificates are not automatically replaced on expiry. On expiry, their state changes from DELIVERED to REPLACE, the monitoring of the certificate stops, and it is possible to delete the certificate from the GUI.

The process to revoke root CA certificates changes the GENERICINTERNAL certificate state to REPLACE. This prompts the security administrator to generate and export a new GENERICINTERNAL certificate.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,* NN10453-100.

2 Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Import Export** link.

The Import/Export window opens.

4 Click the **Generate Cert** link.

The Generate Certificate for Export window opens.

5 Enter the Fully Qualified Domain Name (FQDN) of the component that is being authenticated with the certificate in the **Entity ID** field. This is the device or application which will use the private key for secure communication. The field name has a maximum length of 48 characters. You can only use the following characters in this field:

0-9, a-z, A-Z, period (.) and hyphen (-)

Spaces are not allowed. Additionally, a hyphen (-) cannot be located at the start or at the end of a word.

Example
Allowed: "host-1.com", "host.oz-zo.com"
Not allowed: "-host.com", "host-.com"

6 Enter the IP address (in the form of a.b.c.d) of the entity in the **IP Address** field. The IP address consists of four numbers of 1 to 3 digits, concatenated by 3 dot (".") characters. For example, 192.1.65.20. Only a valid IP address can be entered where the four numbers are between 0-255.

7 Select the entity type from the drop-down list of integrated device types in the **Entity Type** field.

8 Click the **Submit** button.

9 Click the **Confirm** button.

The files are generated to the specified export directory. The default target directory is: /data/NTPkmgr/cert/export. The certificate and private key values are displayed. The certificate chain comprises of CA1_cert.pem, CA2_cert.pem, and the device certificate and private key. These may be exported according to the requirements of the target network element or element manager..

10 Monitor the certificate for expiration by performing the procedure "Managing a GENERICINTERNAL certificate using Certificate Manager" (page 241). After performing this procedure, Certificate Manager begins to monitor the certificate for expiration automatically.

11 You have completed this procedure.

—End—

Generating WEBPKPROXY certificates

Application

Use this procedure to generate and export a WEBPKPROXY certificate. WEBPKPROXY certificates are used for SSL communication used by Apache webserver and Tomcat on the element manager. The WEBPKPROXY certificate replaces self-signed certificates on SPFS devices.

This procedure generates a private key and public key pair. The public key is certified and placed in the certificate. The private key, certificate, CA chain, and trusted certificate are written to the /data/NTPkmgr/cert/export directory on the machine hosting the Certificate Manager.

Note that WEBPKPROXY certificates must be installed manually. When these certificates are first created, they remain in the CREATED state until the certificate is installed. On subsequent creation attempts, WEBPKPROXY certificates change to the DELIVERED state when they have been placed in the /data/pkclient/certificates directory on the element manager.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview,*NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,*NN10453-100.

2 Click the **Import Export** link.

The Import/Export window opens.

3 Click the **Generate Cert** link.

The Generate Certificate for Export window opens.

4 Enter the Fully Qualified Domain Name (FQDN) in the **Entity ID** field of the manager where the certificate will be installed. This is the device or application which will use the private key for secure communication. The field name has a maximum length of 48 characters. You can only use the following characters in this field:

0-9, a-z, A-Z, period (.), hyphen (-)

Spaces are not allowed. Additionally, a hyphen (-) cannot be located at the start or at the end of a word.

Example
Allowed: "host-1.com", "host.oz-zo.com"
Not allowed: "-host.com", "host-.com"

5 Enter the IP address (in the form of a.b.c.d) in the **IP Address** field of the manager where the certificate will be installed. The IP address consists of four numbers of 1 to 3 digits, concatenated by 3 dot (".") characters. For example, 192.1.65.20. Only a valid IP address can be entered where the four numbers are between 0-255.

6 Select the WEBPKPROXY from the drop-down list of integrated device types in the **Entity Type** field. WEBPKPROXY is the default value.

7 Click the **Submit** button.

8 Click the **Confirm** button.

The files are generated to the specified export directory. The default target directory is: /data/NTPkmgr/cert/export. The certificate and private key values are displayed.

Note that HTTP and HTTPS connections continue to be established after certificates expire. This is normal as the communication channel continues to use the certificate for encryption.

9 You have completed this procedure.

—End—

Importing an external certificate using Certificate Manager

Application

Use this procedure to support expiration monitoring of a purchased certificate that is already deployed. When this procedure is complete, the certificate can be viewed and is monitored for expiration by Certificate Manager.

External certificates have a different root CA or trusted anchor to Certificate Manager certificates. There is no impact on external certificates Certificate Manager’s root CA certificate is revoked.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. Secadm group privileges permit you to use all operations in Certificate Manager and secro group privileges permit you only to view and browse in the Certificate Manager tool.

Action

Step Action

At the IEMS workstation

1 Launch the Certificate Manager. Refer to Launching the Certificate Manager in *IEMS Overview*, NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,*NN10453-100.

2 Place the import files in the default import directory. The default certificate import directory for all import types is /data/NTPkmgr/cert/import. The certificate file name must end with the suffix, Ent_cert (for example, host1.us.nortel.comEnt_cert) to be recognized in the Import File drop-down menu. The default certificate import directory is set in the Modify Broker Defaults screen. For more information, see "Configuring the broker default values for Certificate Manager" (page 228).

3 Click the **Import Export** link.

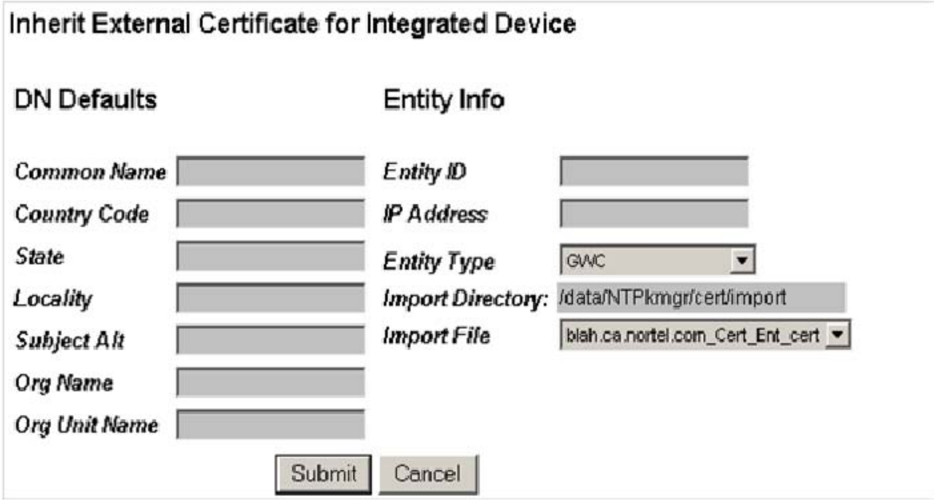
The Import/Export window opens.

4 Click the **Import Cert** link.

The Import window opens.

5 Click the **Inherit Cert (no CSR)** link.

The Inherit External Certificate for Integrated Device window opens.



Inherit External Certificate for Integrated Device

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Unit Name

Entity Info

Entity ID
IP Address
Entity Type: GWC
Import Directory: /data/NTPkmgr/cert/import
Import File: blah.ca.nortel.com_Cert_Ent_cert

The fields in the Inherit External Certificate for Integrated Device window are described in the following table.

Field	Description
DN Defaults	
Common Name	Displays the name of the certificate.
Country Code	Displays the two-character country code according to ISO standard ISO 3166
State	Displays the state.
Locality	Displays the city.
Subject Alt	Displays the IP address of the active unit for the network element or network manager.
Org Name	Displays the organization name.
Org Unit Name	Displays the name of the organization unit.
Entity Info	
Entity ID	Displays the entity ID.
IP Address	Displays the IP address.
Entity Type	Select the entity type from the drop down list.

Field	Description
Import Directory	Displays the import directory.
Import File	Select the certificate from the drop-down list.

6 Select the entity type from the **Entity Type** drop-down list.

7 Select the certificate that you want to import from the **Import File** drop-down list.

8 Click the **Submit** button.

9 You have completed this procedure.

—End—

Revoking a certificate using Certificate Manager

Application

Use this procedure to revoke a device certificate that is monitored by Certificate Manager.

Revoking a WEBPKPROXY certificate requires manual installation of the certificate, otherwise an outage may occur. Revoking a GENERICINTERNAL certificate moves the certificate from a DELIVERED state to a REPLACE state so that the certificate can be deleted and recreated.

> **ATTENTION**
>
> **Possible service outage**
>
> If you are revoking the WEBPKPROXY certificate where the Certificate Manager resides (where the common name in the certificate matches the URL IP address or hostname of the Certificate Manager GUI), then all WEBPKPROXY certificates will be revoked.
>
> Revoking a WEBPKPROXY certificate requires manual installation of the certificate after delivery to successfully activate use of the new certificate, otherwise an outage may result.

> **ATTENTION**
>
> Integrated device certificates that are selectively revoked result in the selective creation and delivery of replacement certificates to their original downstream clients.

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges. You must have secadm and emsadm group privileges.

Action

Step	Action
	At the IEMS workstation
1	Launch the Certificate Manager. Refer to Launching the Certificate Manager. in *IEMS Overview,* NN10329-111 or *Nortel Carrier VoIP IPSec Security Service Implementation Overview,* NN10453-100.
2	Enter your user name and password to log into the Certificate Manager GUI.

3 Click the **Revoke Certificates** link.

The Revoke Certificates window opens.

4 Click the **Revoke Device** link.

A list of certificate types is displayed.

5 Select the devices from the drop-down list for the certificates you want to revoke. Hold down the Ctrl key to select more than one device.

6 Click the **certListing** button.

The Revoke Device Certificate table is displayed.

7 Select your next step.

If the certificate state is	Do
CREATED or DELIVERED	step 8
REPLACE	do not revoke the certificate. There may be a problem communicating with the respective element manager. Resolve the communication problem before going to the next step.

8 Select the check boxes for the certificates you want to revoke.

9 Click the **Revoke** button.

An Operation successful message appears.

10 To ensure that the revoke was successful, view the state of the certificate after 30 minutes. See "Viewing certificates using Certificate Manager".

11 Select your next step.

If the certificate is	Do
DELIVERED	you have completed this procedure
not DELIVERED	there may be a loss of connectivity to the element manager and/or the network element. Verify the alarms at the Certificate Manager and verify the alarms at the element managers.

12 You have completed this procedure.

—End—

Overview of IPSec between IEMS and northbound OSSs

Internet Protocol Security (IPSec) can be used to secure the network path between SPFS servers and northbound OSSs. The IEMS application runs on an SPFS-based server and provides input to the northbound OSS links. You can use IPSec to provide additional protection and encapsulation of IEMS to OSS traffic.

To secure the communications link between IEMS and OSS, you must provision the IPSec security parameters using the Server Security Manager (SSM). The SSM is a component of SPFS and is used to provision and manage IPSec for the SPFS server and all applications that run on the server. You can access the SSM through a web browser.

Configuring IPSec between IEMS and OSS

The following conditions must be met to enable security for a northbound OSS from IEMS:

- Make sure that the IEMS server has software version (I)SN09 or later.
- Enable security on the OSS to secure the connection to the IEMS server.
- Use the SSM to enable security on the IEMS server for communication with the OSS IP address. For each OSS that is provisioned and requires IPSec security, you must create one IPSec entry. For each IPSec entry, there must be a corresponding IKE entry.

  For information on creating IPSec entries, see "Adding an IPSec entry on the IEMS server for communication with OSS" (page 257). For information on creating IKE entries, see "Adding an IKE entry on the IEMS server for communication with OSS" (page 260).

  You can use the SSM interface to secure all network communications, as well as OSS communications. When you are provisioning or deleting security parameters, take care not to disrupt other communication parameters such as telnet or FTP.

IPSec and IKE configuration parameters that are provisioned on the IEMS server must match the corresponding IPSec and IKE parameters on the OSS.

Use the following procedures to configure IPSec between IEMS and the OSS.

- Launching the Server Security Manager. See Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
- "Adding an IPSec entry on the IEMS server for communication with OSS" (page 257)
- "Deleting an IPSec entry on the IEMS server" (page 265)
- "Adding an IKE entry on the IEMS server for communication with OSS" (page 260)
- "Deleting an IKE entry on the IEMS server" (page 266)
- "Adding a transform for an IKE entry on the SPFS server" (page 263)
- "Deleting a transform for an IKE entry on the SPFS server" (page 267)
- "Adding, modifying, or deleting a preshared key for an IKE entry on the SPFS server" (page 268)

Adding an IPSec entry on the IEMS server for communication with OSS

Application

Use this procedure to provision IPSec entries for an IEMS server using the Server Security Manager (SSM).

For each OSS that is provisioned and requires IPSec security, you must create one IPSec entry. For each IPSec entry, there must be a corresponding IKE entry. For information on creating IKE entries, see "Adding an IKE entry on the IEMS server for communication with OSS" (page 260).

Prerequisites

This procedure has the following prerequisites:

- you must have administration privileges

Action

Step	Action
At the IEMS workstation	
1	Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
2	Click the **IPSec Entries** link. *The Server IPSec Entry window opens.*
3	Click the **Add Entry** button. *The Add IPSec Entry window opens.*
4	Configure the IPSec parameter settings to enable secure communication between IEMS and the OSS. IPSec and IKE configuration parameters that are provisioned on the IEMS server must match the corresponding IPSec and IKE parameters on the OSS.

The following table lists the security values for the IPSec entries.

IPSec fields and values

Field	Description	Entry
Remote Address	The source address on incoming packets and the destination address on outgoing packets.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the remote address of the IEMS server.
Remote Port	IP port of the remote system communicating with this server.	1 - 65535, any Enter any.
Local Address	The destination address on incoming packets and the source address on outgoing packets.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the local address of the IEMS server.
Local Port	IP port of this server.	1 - 65535, any Enter any.
Upper Layer Protocol	Determines which protocol traffic this entry is matched against.	any, icmp, tcp, and udp. Enter udp.
Direction	Determines whether this entry is for inbound or outbound traffic.	in, out, and both. Enter both.
Action	Determines the action to take when the traffic pattern is matched.	bypass, drop, and ipsec. Enter ipsec.

Field	Description	Entry
ESP Header ESP Encryption	Describes the encryption algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify that it is present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, NULL, des, and 3des. Enter NULL.
ESP Header ESP Authentication	Describes the authentication algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify that it is present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, sha1, and md5. Enter sha1.
AH Header Authentication Algorithm	Describes the encryption algorithm that will be used to apply the IPSec AH header on outbound datagrams and verify that it is present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, sha1, and md5. Enter none.

5 Click the **Apply** button.

You have completed this procedure.

—End—

Adding an IKE entry on the IEMS server for communication with OSS

Application

Use this procedure to provision IKE entries for an IEMS server using the Server Security Manager (SSM).

Prerequisites

This procedure has the following prerequisites:

- You must have administration privileges.

Action

Step Action

At the IEMS workstation

1 Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.

2 Click the **IKE Entries** link.

The Server IKE Entry window opens.

3 Select **Add Entry** from the drop-down list and click the Go button.

The Add IKE Entry window opens.

4 Configure an IKE entry for each IPSec entry that was provisioned in "Adding an IPSec entry on the IEMS server for communication with OSS" (page 257).

IPSec and IKE configuration parameters that are provisioned on the IEMS server must match the corresponding IPSec and IKE parameters on the OSS.

The following table lists the security values for the IKE entries.

IKE fields

Field	Description	Entry
Remote Address	IP address of the remote system communicating with this server.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the Remote Address which is the address of the OSS as seen by IEMS.

Field	Description	Entry
Local Address	IP address of this server.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the local address which is the address of the IEMS as seen by the OSS.
PFS Group ID	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit). Enter 1.
IPSec Lifetime	Specifies the lifetime for an IPSec Security Association.	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days. Enter 8.
IPSec Lifetime Unit	Specifies the units.	Maximum allowed units in seconds, minutes, hours, or days. Enter hours.
IKE Preshared Key	Specifies the preshared key for this Security Association.	Radio button to select ASCII or hexadecimal. Select ASCII. 20 - 120 character ASCII string. Enter the same key that is entered at the OSS twice.

5 Click the **Apply** button.

You have completed this procedure.

—End—

Adding a transform for an IKE entry on the SPFS server

Application

Use this procedure to add or view transforms for each IKE entry using the Server Security Manager (SSM).

Prerequisites

You must have administration privileges.

Action

Step	Action
At the IEMS workstation	
1	Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
2	Click the **IKE Entries** link. *The Server IKE Entry window opens.*
3	Select **Modify Xforms** from the drop-down list and click **Go**. *The IKE Transforms window opens.*
4	Click the radio button next to the entry you want to change.
5	Click the **Modify** button. *The currently provisioned transforms are displayed.*
6	Click the **Add Xform** button.
7	Select the transform entries. IPSec and IKE configuration parameters that are provisioned on the IEMS server must match the corresponding IPSec and IKE parameters on the OSS.

The following table lists the security values for the IKE transform entries.

IKE fields

Field	Description	Entry
Oakley Group	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.	1 (768-bit), 2 (1024-bit), or 5 (1536-bit). Enter 1.
Authentication Method	The authentication method used for IKE phase 1.	Preshared.
Encryption Algorithm	Specifies the encryption algorithm for a Security Association.	des and 3des. Enter 3des.
Authentication Algorithm	Specifies the authentication algorithm for a Security Association.	sha1 and md5. Enter sha1.
IKE Lifetime	Specifies the lifetime for a IKE phase 1 Security Association.	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days. Enter 8.
IKE Lifetime Unit	Specifies the units.	Maximum allowed units in seconds, minutes, hours, or days. Enter hours.

8 Click the **Apply** button.

An Operation Successful message appears.

You have completed this procedure.

—End—

Deleting an IPSec entry on the IEMS server

Application

Use this procedure to delete an IPSec entry for an IEMS server using the Server Security Manager (SSM).

Prerequisites

You must have administration privileges.

Action

Step	Action
At the IEMS workstation	
1	Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
2	Click the IPSec Entries link. *The Server IPSec Entry window opens.*
3	Click the **Delete Entry** button. *The Delete IPSec Entry window opens.*
4	Select the entry you want to delete by clicking the radio button next to the entry listing.
5	Click the **Delete** button. You have completed this procedure.

—End—

Deleting an IKE entry on the IEMS server

Application

Use this procedure to delete an IKE entry for an IEMS server using the Server Security Manager (SSM).

Prerequisites

You must have administration privileges.

Action

Step	Action
At the IEMS workstation	
1	Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
2	Click the IKE Entries link. *The Server IKE Entry window opens.*
3	Select **Delete Entry** from the drop-down list and click the **Go** button. *The Delete IKE Entry window opens.*
4	Select the entry you want to delete by clicking the radio button next to the entry listing.
5	Click the **Delete** button. You have completed this procedure.

—End—

Deleting a transform for an IKE entry on the SPFS server

Application

Use this procedure to delete a transform for an IKE entry using the Server Security Manager (SSM).

Prerequisites

You must have administration privileges.

Action

Step	Action
At the IEMS workstation	
1	Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.
2	Click the IKE Entries link. *The Server IKE Entry window opens.*
3	Select **Modify Xforms** from the drop-down list. *The IKE Transforms window opens.*
4	Click the radio button next to the IKE entry you want to modify.
5	Click the **Modify** button. *The currently provisioned transforms are displayed.*
6	Click the **Delete Xform** button.
7	Click the radio button next to the transform entry you want to delete.
8	Click the **Delete** button. You have completed this procedure.

—End—

Adding, modifying, or deleting a preshared key for an IKE entry on the SPFS server

Application

Use this procedure to add, delete, or modify a preshared key for each IKE entry using the Server Security Manager (SSM).

Prerequisites

You must have administration privileges.

Action

Step Action

At the IEMS workstation

1 Launch the SSM. Refer to Launching the Server Security Manager in *IEMS Overview*, NN10329-111.

2 Click the **IKE Entries** link.

The Server IKE Entry window opens.

3 Select **Modify Preshared Key** from the drop-down list and click **Go**.

The Change Key window opens.

4 Click the radio button next to the entry you want to modify.

5 Select your next step.

If you want to	Do
change an entry	step 6
add an entry	step 8
delete an entry	step 12

6 Click the **Change** button.

The Change Key window opens.

7 Go to step 9.

8 Click the **Add** button.

The Add Preshared Key window opens.

9 Enter the details for the key.

IPSec and IKE configuration parameters that are provisioned on the IEMS server must match the corresponding IPSec and IKE parameters on the OSS.

The following table lists the security values for the IKE entries.

Field	Description	Entry
IKE Preshared Key	Specifies the preshared key for this Security Association.	Radio button to select ASCII or hexadecimal. Select ASCII. 20 - 120 character ASCII string. Enter the same key that is entered at the OSS twice.

10 Click the **Apply** button.

11 You have completed this procedure.

12 Click the **Delete** button.

The Delete Preshared Key window opens.

13 Click the **Delete** button to confirm the deletion.

14 You have completed this procedure.

—End—

IEMS server startup options

This section describes the procedures for starting and shutting down the IEMS server. After starting the IEMS server successfully, connect the client with the IEMS server. The following sections give the details:

- "Starting the IEMS server" (page 272)
- "Shutting down the IEMS server" (page 276)
- "Viewing the IEMS server status" (page 278)

Starting the IEMS server or changing the IEMS server mode to standby

Application

Use this procedure to start the IEMS server or to put the IEMS into a standby state using the servman from the system where IEMS server is installed.

It also describes the ports which must be opened in the associated firewall.

To start the IEMS server, a valid SSL certificate is required.

Action

Step Action

At the IEMS server system

1 Telnet or switch to the host in which the IEMS server is running.

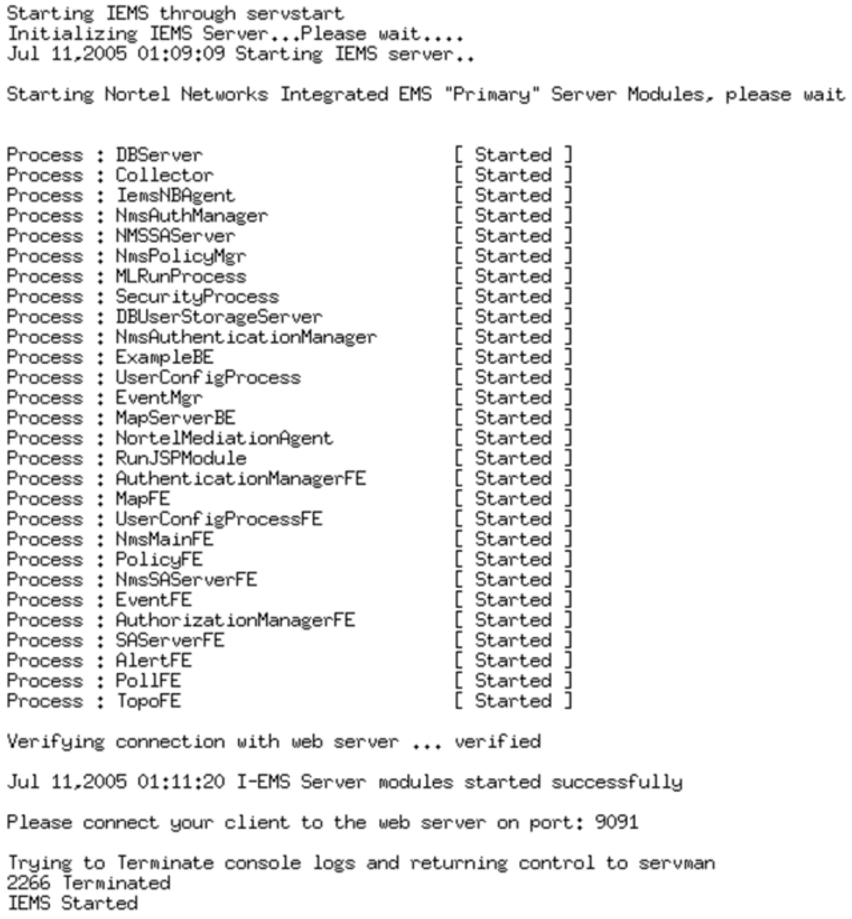
2 Select your next step.

If you want to	go to
start the IEMS server	the next step
put the IEMS server into standby state	step 5

3 Execute the following command to start the IEMS server.

```
/opt/servman/bin/servstart IEMS
```

Servman starts the IEMS with the following message.



```
Starting IEMS through servstart
Initializing IEMS Server...Please wait....
Jul 11,2005 01:09:09 Starting IEMS server..

Starting Nortel Networks Integrated EMS "Primary" Server Modules, please wait


Process : DBServer                          [ Started ]
Process : Collector                         [ Started ]
Process : IemsNBAgent                       [ Started ]
Process : NmsAuthManager                    [ Started ]
Process : NMSSAServer                       [ Started ]
Process : NmsPolicyMgr                      [ Started ]
Process : MLRunProcess                      [ Started ]
Process : SecurityProcess                   [ Started ]
Process : DBUserStorageServer               [ Started ]
Process : NmsAuthenticationManager          [ Started ]
Process : ExampleBE                         [ Started ]
Process : UserConfigProcess                 [ Started ]
Process : EventMgr                          [ Started ]
Process : MapServerBE                       [ Started ]
Process : NortelMediationAgent              [ Started ]
Process : RunJSPModule                      [ Started ]
Process : AuthenticationManagerFE           [ Started ]
Process : MapFE                             [ Started ]
Process : UserConfigProcessFE               [ Started ]
Process : NmsMainFE                         [ Started ]
Process : PolicyFE                          [ Started ]
Process : NmsSAServerFE                     [ Started ]
Process : EventFE                           [ Started ]
Process : AuthorizationManagerFE            [ Started ]
Process : SAServerFE                        [ Started ]
Process : AlertFE                           [ Started ]
Process : PollFE                            [ Started ]
Process : TopoFE                            [ Started ]

Verifying connection with web server ... verified

Jul 11,2005 01:11:20 I-EMS Server modules started successfully

Please connect your client to the web server on port: 9091

Trying to Terminate console logs and returning control to servman
2266 Terminated
IEMS Started
```

4 You have completed this procedure.

5 Execute the following command to put the IEMS server into standby state:

`servstandby iems`

Servman places the active IEMS server in standby mode and switches the inactive IEMS server to active mode. The following output appears for the inactive IEMS server:

```
Initializing IEMS Server in Stanby mode...Please
wait....
Jul 28,2006 09:20:56 Certificate check done
Jul 28,2006 09:20:56 Taking server to standby mode
Jul 28,2006 09:20:56 Getting VIP
IEMS is in STANDBY STATE ...........
Trying to Terminate console logs and returning control
to servman
4249 Terminated
```

6 You have completed this procedure.

—End—

The ports listed in the following table must be opened in the associated firewall.

The CEM ports listed in the following table must be opened if the CEM is added to IEMS topology.

Ports occupied by processes which must be opened in the associated firewall

Process	Port	Protocol	Connection request direction	Associated software
FTP/SFTP for performance	21	FTP	Outgoing	IEMS
SSH	22	TCP	Incoming	IEMS
Syslog client	514	UDP	Outgoing	IEMS
LDAPS	636	TCP	Incoming	Security Server
Token Admin GUI (SSL mode)	8443	TCP	Incoming	Security Server
NT STD Export	8555	TCP	Incoming	IEMS
SCC2 Export	8556	TCP	Incoming	IEMS
Client Server Communication port [Primary]	9004	TCP	Incoming	IEMS
Client Server Communication port [Secondary]	9005	TCP	Incoming	IEMS
IEMS Server HTTPS mode	9091 (defa ult)	SSL	Incoming	IEMS
Server EM Adapter	22396	TCP	Incoming	CEM
Telnet FTP Handler	22397	TCP	Both incoming and outgoing	CEM
Telnet FTP Handler	22398	TCP	Both incoming and outgoing	CEM
EM Adapter	22401	TCP	Incoming	CEM
Alarm Exporter	22403	TCP	Incoming	CEM
Config Broker	22405	TCP	Incoming	CEM
Security Server SunONE IS (SSL)	58081	TCP	Incoming	Security Server

The IEMS server connects in the SSL mode (port 9091) only if the SSL certificate is available.

Shutting down the IEMS server

Application

The IEMS 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.

Action

The following sequence of operations takes place during the IEMS server shutdown process:

Step **Action**

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 IEMS).

6 Exit (the main process).

To shut down the IEMS 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.

—End—

Shutting down the IEMS 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 the 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 IEMS server status

Application

Use this procedure to check the IEMS server status using the servman from the system where IEMS server is installed.

Action

Step Action

At the IEMS server workstation

1 Telnet or switch to the host in which IEMS server is running.

2 Execute the following command to view the status of the IEMS server.

```
/opt/servman/bin/servquery -status -g IEMS
```

If the IEMS server is running, the following message is displayed.

```
IEMS
=====
Executing:  /opt/nortel/iems/current/bin/IEMSHealthS
tatus.sh
IEMS Instance is UP
```

If the IEMS server is on standby, the following message is displayed.

```
IEMS
=====
Executing:  /opt/nortel/iems/current/bin/IEMSHealthS
tatus.sh
IEMS Instance is in STANDBY state
```

If the IEMS server is not running, the following message is displayed.

```
IEMS
=====
Executing:  /opt/nortel/iems/current/bin/IEMSHealthS
tatus.sh
IEMS Instance is DOWN
```

3 You have completed this procedure.

—End—

Administering fault operations

IEMS administrator can configure the event filter, alarm filter, and event cleanup interval. In addition, the administrator can change the attributes for SNMP fault feeds.

Configuring event filters

Application

Use this procedure to configure the event filter and event filter actions.

Event filters are configured to automate actions for selected events. For an event, all event filters in the event filters list are tested to see if they satisfy the match criteria. If the event matches an event filter, then the actions associated with that filter (for example, e-mail, suppressing the event, generating traps, or custom filter action) are executed. Then the event is re-checked with the remaining event filters on the list. If a match is found, the corresponding event filter is executed.

You can set the order of the event filters and filter actions by dragging and dropping the filters in the Event Filter List and the Configured Actions list.

Defining an event filter involves the following steps:

- Select the events for which necessary action has to be initiated.
  - Specify the Match Criteria - Source, Entity, Category, Severity, and others.
- Specify the actions to be taken for events that match the criteria.

Action

Step Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *IEMS Overview*, NN10329-111.

2 Select the **Network Events** node under the Fault Management node in the IEMS client.

3 Select the **Edit-->Configure-->Event Filters** menu item to open the Event Filter Configuration user interface.

The Event Filter Configuration window opens.

4 Select your next step.

If you want to	Do
add an event filter	step 5
modify an event filter	step 7
add a filter action	step 12

If you want to	Do
modify a filter action	step 15
delete a filter action	step 23
delete an event filter	step 28
save to file	step 31
load from file	step 35

5 Click the **Add** button under Event Filter.

6 Enter a filter name in the Filter Name field and go to step 9.

7 Select the filter you want to modify in the Configured Filter List.

8 Click the **Modify** button under Event Filter.

9 Set the match criteria as required. The match criteria determines whether the incoming event is filtered or not. If the field is blank, it is automatically matched. All match criteria specified must be satisfied for the filter to be applied. For more information on setting match criteria, see "Setting match criteria" (page 283).

10 Click the **More** button to enter user properties and trap-based criteria.

11 Select your next step.

you are	Do
adding an event filter	go to the next step
modifying the event filter	go to step 20

12 Ensure that the filter is selected in the Configured Filter list and click the **Add** button under Filter Action to associate at least one action with the event filter.

At least one filter action must be associated with the event filter.

13 Enable a radio button under Action Type. The action types are listed in the following table.

Action type	Description
Suppress Action	Allows you to suppress events that match the filter criteria.

Action type	Description
Run Command Action	Allows you to run a command on the IEMS server platform if the incoming event has matching filter criteria.
Send Trap Action	Allows you to send SNMP V1/V2c traps for events matching the filter criteria.
Send E-Mail Action	Allows you to send an e-mail for events matching the filter criteria.
Custom Filter	Allows you to use your own Java code to filter events and perform actions.

14 Go to step 18.

15 Select the filter you want to modify in the Configured Filter List.

16 Select the action you want to modify under Configured Actions.

17 Click the **Modify** button under Filter Action.

18 Enter the action details under Filter Action Details.

19 Click the **Update Action** button. If you are modifying the action, go to step 21.

20 Click the **Update Filter** button to update the filter.

21 Repeat step 12 to step 20 to add additional filter actions if required.

22 You have completed this procedure.

23 Select the event filter in the Configured Filter list and select the action you want to delete under Configured Actions.

24 Click the **Delete** button under Filter Action.

25 Click the **Yes** button in the confirmation dialog box.

26 You have completed this procedure.

27 Select the event filter you want to delete under Configured Filter List.

28 Click the **Delete** button under Event Filter.

29 Click the **Yes** button in the confirmation dialog box.

30 You have completed this procedure.

31 To save the event filter, select the event filter you want to save under Configured Filter List and click the **Save to File** button.

32 You have completed this procedure.

33 Enter the path and filename where you want to save the file and click the **Save** button.

34 You have completed this procedure.

35 To add an existing event filter to the list of event filters, click the **Load From File** button.

36 Enter the file on the server that you want to load and click the **Load** button.

37 Click the **Apply** button.

38 You have completed this procedure.

—End—

Setting match criteria

See the following table for details of the match criteria.

Match criteria	Description
Filter name	Enter the name of the filter.
Severity	Enter the match criteria based on the severity of the event (Critical, Major, Minor, Warning, Info).
Message	Enter a message for the incoming event.
Category	Enter a category name. This can be used to organize events, for example, communication, environmental.
Node	Enter the name of the device.
Entity	Enter information for the device in which the problem has occurred.

Match criteria	Description
Source	Use this field to filter out events matching a source.
Note: You can use the following expressions to specify the match criteria. Asterisk (*): use as a wildcard to specify a match with any character Exclamation (!): use at the start of a field to exclude events matching this expression. Comma (,): use to separate multiple values in one search string.	

To use the event filter, enter the name of the event filter followed by its match criteria. 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 the event's base properties as match criteria such as groupname, helpURL, id, and time in the More option. Thus, the More option serves for both Event's base properties as well as user properties.

Enable or disable event filters

Event Filters can be enabled or disabled by using the parameter "enable" in the event.filters file present in the /opt/nortel/iems/current/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", the filter is disabled.

Example

```
<EVENT_FILTERS>

<FILTER

name="MyEventFilter"

enable="true">

<FILTER_ACTIONclassName="com.adventnet.nms.eventdb.UserFilter"

name="userprop"

userclass="com.adventnet.nms.eventdb.UserFilter" />

</FILTER>

</EVENT_FILTERS>
```

You can only enable or disable event filters by editing the event.filters file. This is not available through the Event Filter Configuration Interface.

Configuring alert filters

Application

Use this procedure to configure alert filters and alert filter actions using the Alert Filter Configuration tool.

Events are correlated into alarms (also known as alerts). They represent the current status of the existing problems in a network. An alert filter executes certain corrective actions whenever alarms are received with configurable searching criteria, such as suppressing multiple alarms in a given interval, running shell commands on the server system, sending e-mails, sending traps, and running custom code to filter alarms.

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 alarm is completed.

An alert filter can be configured using the Alert filter configuration tool. 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.

Action

Step Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *IEMS Overview*, NN10329-111.

2 Select the **Alarms** node under the Fault Management node of the IEMS client tree.

3 Click the **Edit** menu command and select **Edit-->Configure-->Alarm Filters** (Ctrl+Shift+A).

The Alert filter configuration window is displayed.

4 Select your next step.

If you want to	Do
add an alert filter	step 5
modify an alert filter	step 7
add a filter action	step 14

If you want to	Do
modify a filter action	step 17
delete a filter action	step 25
delete an alert filter	step 29
save to file	step 33
load from file	step 36

5 Click the **Add** button under Alert filter.

6 Enter a name for the filter in the Alert filter name field and go to step 9.

7 Select the filter you want to modify under Configured filters.

8 Click the **Modify** button under Alert filter.

9 Set the match criteria as required. The match criteria determines whether the incoming alert is filtered or not. If the field is blank, it is automatically matched. All match criteria must be satisfied for the filter to be applied. For information on each of the match criteria fields, see "Setting match criteria" (page 288).

10 Click the **More** button of the Alert filter configuration tool GUI.

11 Specify the **Property Name** and **Match Criteria**. While specifying the additional criteria, specify only those properties that are in the alarm.The name must exactly match the case of the alarm.You can also add the alarm base properties for match criteria, such as group name, help URL, ID, and time.

12 Click the **OK** button.

13 Select your next step.

If you are	Do
adding an alert filter	the next step
modifying the alert filter	step 22

14 Ensure that the alert filter you want to modify is selected under Configured filters and click the **Add** button under Action filter action to associate at least one filter action with the alert filter.

At least one filter action must be associated with the alert filter.

15 Enable a radio button under Action type. The action types are listed in the following table. For more details see "Filter action details" (page 289).

Action type	Description
Suppress Action	Allows you to suppress alerts that match the filter criteria.
Run Command Action	Allows you to run a command on the IEMS server platform if the incoming alert has matching filter criteria.
Send Trap Action	Allows you to send SNMP V1/V2c traps for alerts matching the filter criteria.
Send E-Mail Action	Allows you to send an e-mail for alerts matching the filter criteria.
Custom Filter	Allows you to use your own Java code to filter alerts and perform actions.

16 Go to step 20.

17 Select the filter you want to modify in the Configured filters list.

18 Select the action you want to modify under Configured filter actions.

19 Click the **Modify** button under Filter action.

20 Enter the action details under Action details.

21 Click the **Update action** button. If you are modifying the action, go to step 23.

22 Click the **Update filter** button to update the filter.

23 Repeat step 14 to step 22 to add additional filter actions if required.

24 You have completed this procedure.

25 Select the action you want to delete under Configured filter actions.

26 Click the **Delete** button under Alert filter action.

27 Click the **Yes** button in the confirmation dialog box.

28 You have completed this procedure.

29 Select the alert filter you want to delete under Configured filters.

30 Click the **Delete** button under Alert filter.

31 Click the **Yes** button in the confirmation dialog box.

32 You have completed this procedure.

33 To save the alert filter, select the alert filter you want to save under Configured filters and click the **Save to file** button.

34 Enter the path and filename where you want to save the file and click the **Save** button.

35 You have completed this procedure.

36 To add an existing alert filter to the list of alert filters, click the **Load from file** button.

37 Enter the file on the server that you want to load and click the **Load** button.

Any filter with the same match criteria as that of an existing filter currently listed in the Configured filters list is replaced with the alert filter from the file that you load.

38 Click the **Apply** button.

39 You have completed this procedure.

—End—

Setting match criteria

The values that you specify in the match criteria fields determines whether the incoming alarm need to be filtered or not. If this field is empty, it is matched automatically. For the alert filter to be applied, all the match criteria specified must be satisfied. If even one criterion fails, the filter is not applied. The following table lists the match criteria.

Field	Description
Alert filter name	Enter the name of the filter.
Severity	The match criteria is based on the severity of the alarm, such as Critical, Major.

Field	Description
Message	The match criteria is based on a message of the incoming alarm, such as Interface failure, Status Poll failed. Click **Message**.The Alert filter message dialog box is displayed. Enter the message.
Category	The match criteria is based on an alarm object property with a category name to which the alarm belongs. This is used to organize alarms.
Entity	The match criteria is based on the information about an exact device in which a problem has occurred.

Filter action details

IEMS supports the following types of alert filter actions:

Field	Description
Suppress Action	
Suppress Action Name	Enter 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	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 Action	
Send Trap Action Name	Enter a name for the filter action.
Trap Destination	The destination host to which the trap is to be sent.
Destination Port	The destination port to which the trap is to be sent.
Trap Community	The community for the trap to be sent.
Enterprise	The OID of the trap. This is only applicable for SNMP V1 traps alone.
Generic Type	The number to be used for the trap.This is only applicable for SNMP V1 traps alone.

Field	Description
Specific Type	The number to be used for the trap.This is only applicable for SNMP V1 traps alone.
SysUpTime(secs)	The sysuptime value to be used in the trap.
Variable Bindings List	Click **Add** in the 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 Action	
Send E-mail Action Name	Enter a name for the filter action.
SMTP Server	The SMTP server address.
Recipient’s Address	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	The sender’s address from which the e-mail is to be sent.
Subject	The subject of the mail.
Message	The message to be emailed.
Run Command Action	
Run Command Action Name	Enter a name for the filter action.
Run Command	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 lists all the directories available under /opt/nortel/iems/current.

Field	Description
Command Results	This field contains two options. **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	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	
Custom Filter Action Name	The name for the filter action.
Custom Filter Class Name	The custom filter’s class name.

Enabling and disabling alarm filters

The configured alert filter can be enabled or disabled using the enable parameter in the alert.filters file located in the /opt/nortel/iems/current/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 the Alarm Filter can be done only by editing the alert.filters file and not through the Alert Filter Configuration tool.

Configuring the destination for SNMP traps

Application

Use this procedure to configure the destination for SNMP traps on the Integrated Element Management System (IEMS) server and other Server Platform Foundation Software (SPFS) based servers that need to forward their SNMP traps to the Integrated Element Management System (IEMS) 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 (IEMS) resides

  You can obtain the IEMS IP address to use as the destination for SNMP traps, by logging in to the IEMS server and executing the command "getpip.ksh IEMS".

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

1 Log in to the SPFS-based server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

`IP address` is the IP address of the SPFS-based 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 -
```

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 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup 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 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON 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:  45.123.45
6.78):
```

10 When prompted, enter the IP address of the server where the IEMS resides, or press the Enter key to accept the default if one is specified.

You can obtain the IEMS IP address to use as the destination for SNMP traps, by logging in to the IEMS 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 return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring the Event Cleanup interval

Application

Use this procedure to configure the Event Cleanup interval in the IEMS client.

The events in the IEMS database are cleaned up in the regular intervals specified.

The default Event Cleanup Interval is 7 days.

Action

Step	Action
At the IEMS workstation	
1	Launch the IEMS Java Web Start Client. Refer to "Launching the IEMS Java Web Start Client" in *IEMS Overview*, 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.
5	You have completed this procedure.

—End—

Changing attributes for SNMP fault feeds

Application

Use this procedure to change the SNMP and SNMP v3 attributes for SNMP northbound fault feeds using the IEMS Configuration tool (iems_config.sh).

IEMS stores these attributes in the /opt/nortel/iems/current/conf/NM-SProcessesBE.conf configuration file (for SNMP attributes) and the /opt/nortel/iems/current/conf/mediationagent/v3entries.xml file (for SNMP v3 attributes). The attributes apply only to the IEMS SNMP northbound interface. The attributes are changed using the IEMS Configuration tool (iems_config.sh).

ATTENTION

Editing the resource description format attribute affects the NB SNMP OSS feeds. This feature is intended as controlled availability for (I)SN08, (I)SN09, and (I)SN09U. If you want to modify the NB SNMP agent, contact Nortel System Engineering.
This feature is not included in the (I)SN09U OSS guide, PLN-i09U-OSS, but Service Bulletin 020665-01 includes details of this feature.

Action

Step Action

At the IEMS 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 server where IEMS resides

2 When prompted, enter your user ID and password.

3 Run the iems_config.sh file located in the <IEMS Home>/bin directory.

The following menu appears.

```
1 Configure OfficeName
2 Configure TableSpace
3 Configure IEMS NB SNMP Agent
X Exit
```

4 Enter the number next to the Configure IEMS NB SNMP Agent menu option to configure the IEMS NB SNMP Agent.

Example response

```
Configure the Agent Settings:
-----------------------------
(0) Exit
(1) View
(2) Edit
Enter your Choice:
```

5 Select your next step.

If you want to	Do
view the agent settings	the next step
edit the agent settings	go to step 8

6 Enter the number next to the View menu option to view the agent settings.

Example response

```
Showing the Agent Settings
-----------------------------
The Snmp Agent Port is :  8001
The Snmp Version is    : v2c
The Communities are    : public
The Resource Description:  0 (0- IEMS=source;componentI
d ; 1 - neType=EquipmentId;componentId)
```

7 You have completed this procedure.

8 Enter the number next to the Edit menu option to edit the SNMP agent settings.

Example response

```
Choose the Configuration you wish to change
(0) Exit
(1) Agent Port
(2) Agent Version
(3) Agent Community
(4) Vacm
(5) The ResourceDescription format
(6) All
Enter your Choice :
```

9 Select your next step.

If you want to	Do
edit all SNMP attributes	go to the next step
edit the agent port attribute	go to step 15
edit the agent version attribute	go to step 18
edit the agent community attribute	go to step 21
edit SNMP v3 attributes (Vacm)	go to step 23
edit the resource description format attribute	go to step 34

10 Enter the number next to the "All" option to edit all the SNMP attributes.

Example response

```
Agent Port(0 - 65535):
```

11 Enter the required agent port. The Agent Port must be within the range 0-65535. The default value is 8001.

Example response

```
Snmp Agent Version (v2c/v3):
```

12 Enter the agent version.

Example response

```
Communities separated by ";":
```

13 Enter the community string. If you are entering more than one community string, separate them using a semicolon (;). The default value is public.

Example response

```
Completed Modifying the Settings
!!!!  Agent has to restarted for the changes made!!!!
```

14 You have completed this procedure.

15 Enter the number next to the "Agent Port" option in the menu.

Example response

```
Agent Port(0 - 65535):
```

16 Enter the required agent port. The Agent Port must be within the range 0-65535.

Example response

```
Completed Modifying the Settings
```

```
!!!!  Agent has to restarted for the changes made!!!!
```

17 You have completed this procedure.

18 Enter the number next to the "Agent Version" option in the menu.

Example response

```
Snmp Agent Version (v1/v2c/v3):
```

19 Enter the agent version.

Example response

```
Completed Modifying the Settings
!!!!  Agent has to restarted for the changes made!!!!
```

20 You have completed this procedure.

21 Enter the number next to the "Agent Community" option in the menu.

Example response

```
Communities separated by ";":
```

22 Enter the community string. If you are entering more than one community string, separate them using a semicolon (;).

Example response

```
Completed Modifying the Settings
!!!!  Agent has to restarted for the changes made!!!!
```

23 To change the SNMP v3 attributes, enter the number next to the "Vacm" option in the menu.

The SNMP version of SNMP northbound fault feed must be v3 to change the SNMP v3 vacm attributes. If the version is not v3, a "Change the Version before configuring Vacm" message is displayed and prompts you to change the SNMP version.

Example response

```
Enable VACM <Y/N> :
```

24 Enter **Y** to enable VACM.

Example response

```
*********** V3 Settings *********
Do you need the V3 USMUser Configurations to be
Modified?  <Y/N>
```

25 Enter **Y** to modify the V3 USMUser Configurations.

Example response

```
Configure the USMUserTable Entries
```

```
Available options
<1> Add
<2> View
<3> Edit
<0> Exit
Enter your Choice :
```

26 Follow the prompts to edit the V3 USMUser Configurations and then select the number next to Exit in the Configure the USMUserTable Entries menu.

Example response

```
Configuring the VACM Tables
Do you need the VACM Configurations to be Modified
<Y/N> :
```

27 Enter **Y** to modify the VACM Tables.

Example response

```
Configure the VacmContextTable Entries
Available options
<1> Add
<2> View
<3> Edit
<0> Exit
Enter your Choice :
```

28 Follow the prompts to modify or view the VacmContextTable entries and then select the number next to Exit in the Configure the VacmContextTable Entries menu.

Example response

```
Configure the VacmAccessTable Entries
Available options
<1> Add
<2> View
<3> Edit
<0> Exit
Enter your Choice :
```

29 Follow the prompts to modify the VacmAccessTable entries and then select the number next to Exit in the Configure the VacmAccessTable Entries menu.

Example response

```
Configure the VacmGroupTable Entries
Available options
<1> Add
<2> View
<3> Edit
```

```
<0> Exit
Enter your Choice :
```

30 Follow the prompts to modify the VacmGroupTable entries and then select the number next to Exit in the Configure the VacmGroupTable Entries menu.

Example response

```
Configure the VacmFamilyTable Entries
Available options
<1> Add
<2> View
<3> Edit
<0> Exit
Enter your Choice :
```

31 Follow the prompts to modify the VacmGroupTable entries and then select the number next to Exit in the Configure the VacmFamilyTable Entries menu.

Example response

```
Completed Modifying the Settings
!!!!  Agent has to restarted for the changes made!!!!
```

32 Enter **Y** to restart the agent.

```
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".

33 You have completed this procedure.

34 Enter the number next to the "ResourceDescription format" option in the menu.

Example response

```
The ResourceDescription Format (0 - IEMS=source;compone
ntID ; 1 - neType=EquipmentId;componentId) ";" :
```

35 Select option 1 to update the resource description format.

Example response

```
The ResourceDescription Format (0 - IEMS=source;compone
ntID ; 1 - neType=EquipmentId;componentId) ";" :  1
Completed Modifying the Settings
!!!!  Agent has to restarted for the changes made!!!!
Would you like to restart the Agent for the changes to
take effect (Y/N) :
```

36 Enter **Y** to restart the agent.

37 You have completed this procedure.

—End—

Using other administrative operations

The IEMS administrator can configure 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.

Viewing audit and security logs

IEMS 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 audit and security log messages are stored in the log files of /var/log/auditlog and /var/log/securitylog respectively. This subsection provides procedures on how to view both the audit and security logs from the client GUI.

Viewing audit logs

Application

Use this procedure to view audit logs.

Action

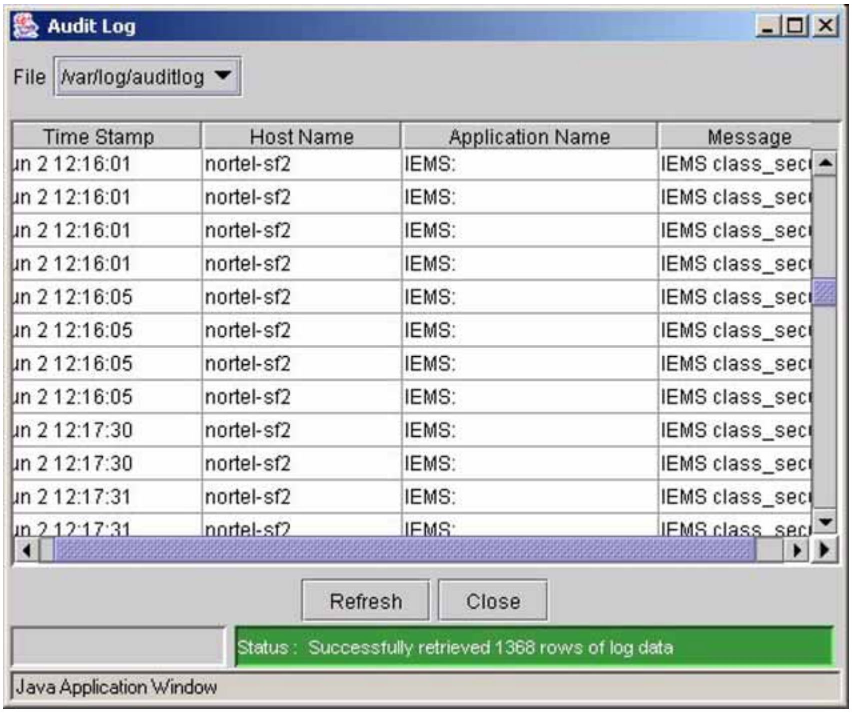
Step Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to Launching the IEMS Java Web Start Client in *IEMS Overview*, NN10329-111.

2 Select the **Tools-->Audit Logs** menu command to view the audit logs.

The Audit Log window (as shown below) is displayed. Following the window is a table with definitions of its attributes.



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

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 IEMS is running.
Application Name	This indicates the name of the application (running on SPFS) for which the logs are generated.
Message	The log message, which indicates the state of the executing operation.

3 You have completed this procedure.

—End—

Viewing security logs

Application

Use this procedure to view security logs.

Action

Step	Action

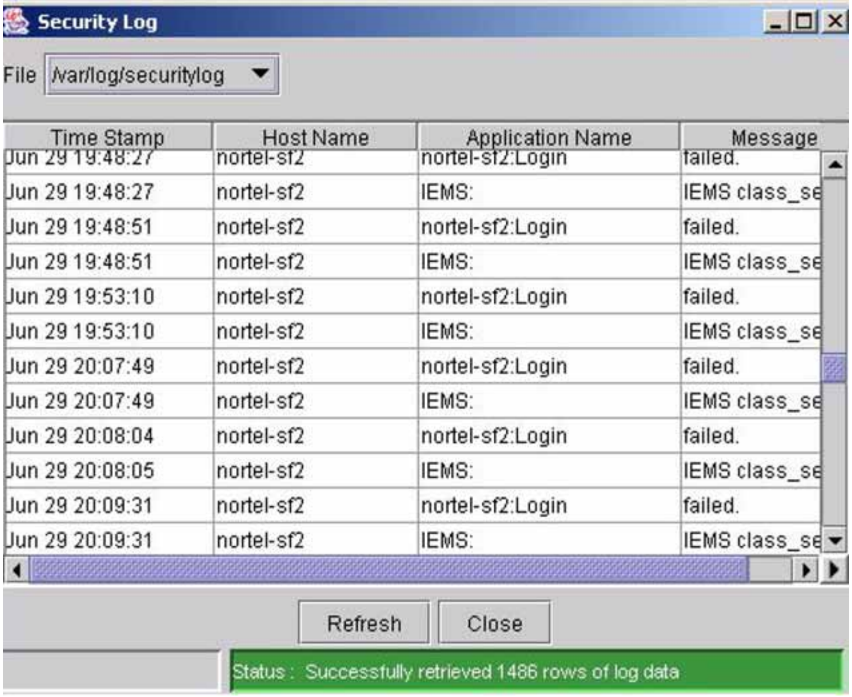
At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to Launching the IEMS Java Web Start Client in *IEMS Overview*, NN10329-111.

2 Select the **Tools-->Security Logs** menu command to view the security logs.

The Security Log window as shown below is displayed.

The descriptions of the fields in the Security Log window are the 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

3 You have completed this procedure.

—End—

Configuring the client retry time

Application

Use this procedure to configure the client retry time.

When the IEMS server stop or shutdown in unforeseen circumstances, the IEMS Java Web Start Client tries to reconnect the IEMS server for a certain period. This period is known as the client retry time. The client retry time is modified by changing the value for MAX_RETRY_PERIOD parameter in clientparametes.conf file present under the /opt/nortel/iems/current/conf directory.

Action

Step **Action**

At the IEMS workstation

1 Switch to the /opt/nortel/iems/current/conf directory in the system where the IEMS 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 IEMS server to implement the changes.

6 You have completed this procedure.

—End—

Changing the security notice text

Application

Use this procedure to change the security notice text.

After you log in (using the Authentication dialog), the system displays a splash screen, then the Security Notice window. IEMS stores the Security Notice text in the editable file securitywarning.txt (present under /opt/nortel/iems/current/conf directory where the IEMS server is installed).

Action

Step	Action
At the IEMS workstation	
1	Switch to the /opt/nortel/iems/current/conf directory in the system where the IEMS 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 IEMS Server to implement the changes. After modifying the text in securitywarning.txt file, the IEMS server must be restarted.
6	You have completed this procedure.

—End—

Configuring the printer

Application

Use this procedure to configure a network printer so that you can print from the IEMS server.

The print command in the IEMS client provides the ability to print a selected set of alarms or events from the IEMS alarms and event browsers. The output of this print command is spooled to the default system printer which is configured on the IEMS SPFS server.

To enable the print command capability, it is required that the craftsperson configure a default printer on their IEMS SPFS server. You can configure the printer by using standard Solaris unix commands.

The system saves and prints only the current range of alarms or events in the selected alarms or events panel of the IEMS client.

Prerequisites

To perform this procedure, you must have root user privileges.

Action

Step Action

At your workstation

1 Telnet to the active IEMS server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server where IEMS 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 Determine whether a default printer is configured on the IEMS SPFS server by typing:

```
lpstat -d
```

and pressing the Enter key.

If a default system printer is configured, the system returns the system default destination, for example:

```
system default destination:  zcort0r1:pc3214b
```

If a default system printer is not configured, the system returns the following response:

```
no system default desintation
```

If	Do...
you want to use the current default system printer	step 8
you want to use a different default system printer	step 6
no default system printer is configured	step 6

6 Configure a default system printer, by typing:

```
lpadmin -d <server:printer destination>
```

and pressing the Enter key.

Example

```
lpadmin -d PRTPP05P:pnc0p02c
```

For detailed information, view the man pages for the lpadmin command by entering:

```
man lpadmin
```

If you want to set up more advanced options with respect to printing, please contact your unix system administrator.

To confirm the printer is set as the default system printer, repeat step 5.

7 Log out of the IEMS server.

The IEMS is configured with a default system printer. If you issue the print command, the set of alarms or events from the IEMS client results in the associated print request being spooled to the default system printer on the IEMS SPFS server.

8 You have completed this procedure.

—End—

Configuring the office name

Application

Use this procedure to configure the office name.

The office name is the name of the host where the IEMS is running. It is displayed in the title bar of the IEMS client. You can configure the office name to any suitable name by using the *iems_config.sh* tool located in the /opt/nortel/iems/current/bin directory.

Prerequisites

To perform this procedure, you must have root user administration privileges.

Action

Step Action

At the IEMS server

1 Run the iems_config.sh file located in /opt/nortel/iems/current/bin directory.

The following list of options are displayed.

```
1 Configure OfficeName
2 Configure TableSpace
3 Configure IEMS NB SNMP Agent
X Exit
```

2 Type "1" and press the Enter key to select the **Configure OfficeName** option.

The following query for entering the office name is displayed:

```
Please enter the office name:
```

3 Enter the office name you want to be displayed in the IEMS client.

On successfully updating the office name, the following message is displayed:

```
Successfully updated the office name in the IEMS
installation.
1 Configure OfficeName
2 Configure TableSpace
3 Configure IEMS NB SNMP Agent
X Exit
```

4 Re-start the IEMS client for the change of office name to appear in the client title bar.

5 You have completed this procedure.

—End—

Using the Runtime Administration tool

The Runtime Administration tool helps you to administer IEMS modules at runtime. By configuring the system at runtime using this tool, you avoid having to restart the IEMS server every time a configuration is performed. This tool can be accessed though the menu command **Tools-->Runtime Administration**.

The descriptions of the toolbar buttons of the Runtime Administration tool are in the following table:

Toolbar button	Description
💾	This tool button is used to save configuration changes performed through the Runtime Administration GUI in the IEMS 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:

- Configuring SCC2 Northbound Fault Feeds
- Configuring SNMP Northbound Fault Feeds
- Configuring SYSLOG Customerlog Configuration
- Configuring NTSTD Northbound Fault Feeds

For configuring northbound fault feeds, refer to *IEMS Fault Management*, NN10334-911.

Refer to the following sections for configuring log settings:

- "Configuring log settings" (page 316)

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 /opt/nortel/iems/current/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 the IEMS. Using this tool, update the file at runtime so that IEMS server restart is not required after configuration.

The Runtime Administration Tool can be used to configure the Server-related log messages only. To configure Client-related logs, manually configure the logging_parameters.conf file located in the /opt/nortel/iems/current/conf directory.

This subsection describes the procedures for the following tasks:

- "Opening the Logging Configuration GUI" (page 316)
- "Adding log files" (page 317)
- "Viewing details of log files" (page 319)
- "Modifying log file details" (page 319)

Opening the Logging Configuration GUI

Application

Use this procedure to open the Logging Configuration GUI.

Action

Step Action

At the IEMS workstation

1 Launch the IEMS client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.

3 Select the **Log Settings** node under the Miscellaneous tree.

The Logging Configuration GUI is displayed in the right hand side frame.

4 You have completed this procedure.

—End—

Adding log files

Application

Use this procedure to add new log files.

Action

Step	Action

At the IEMS workstation

1 Refer to the "Opening the Logging Configuration GUI" (page 316) section to open the Logging Configuration GUI.

2 Specify the name of the log file in Log File Name field.

Only a file name that are compatible with an OS is 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 the Logging Directory field.

By default, the log files are stored in /opt/nortel/iems/current/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 /opt/nortel/iems/current and the new log file is stored in this location. If logs/newlogdir is specified, a new directory is created in the /opt/nortel/iems/current/logs directory.

4 Specify the number of lines to be written in the log file in the 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

When the log file exceeds the maximum number of lines specified, it is carried forward to another new file that is created with a similar name. For example, when newfile.txt reaches 10000 lines, then a new file newfile1.txt is created and the logging continues.

5 Specify the number of files that can be created at such cases in the 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 the Maximum Lines Cached field.

For example, if the value is set as 50, the first 50 lines are 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?** check box if the time stamp is required along with log messages.

8 Click the **Next** button.

9 Type the unique key name in the Key Name field.

This serves as the key with which IEMS 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 the 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 a 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 as follows.

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 are recorded.

13 To enable the logging in this new log file, check the **Enable Logging?** check box.

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.

16 You have completed this procedure.

—End—

Viewing details of log files

Application

Use this procedure to view details of log files.

Action

Step Action

At the IEMS workstation

1 Refer to the "Opening the Logging Configuration GUI" (page 316) procedure 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.

4 You have completed this procedure.

—End—

Modifying log file details

Application

Use this procedure to modify log file details.

Action

Step	Action
	At the IEMS workstation
1	Refer to the "Opening the Logging Configuration GUI" (page 316) procedure 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" (page 317)section.
5	Click the **Finish** button.
6	You have completed this procedure.

—End—

Administering IEMS with Web Client

In IEMS Web Client, you can do the following:

- view server logs
- configure log settings
- configure user settings

Viewing server logs in Web Client

Application

Use this procedure to view server logs.

The logs are essential for debugging, recovery of server, or viewing error messages. In IEMS Web Client, you can view the logs easily. To view the server logs, connecting to the server terminal is not required.

Action

Step Action

At the IEMS workstation

1 Refer to the "Launching IEMS Web Client" to launch the IEMS 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.

5 You have completed this procedure.

—End—

Configuring log settings in Web Client

The Logging Service can be used for pinpointing bugs, configuration errors, performance blockades, creating audit logs, and keeping track of actions on 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 /opt/nortel/iems/current/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.

This subsection contains two procedures:

- configuring log settings
- configuring the logging levels for the modules

Configuring log settings

Application

Use this procedure to configure the log settings in Web Client.

Action

Step	Action
At the IEMS workstation	
1	Refer to "Launching IEMS Web Client" to launch the IEMS 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 a 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 IEMS 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 of 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, 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 IEMS modules such as Map, Topology, Provisioning, etc.

5 You have completed this procedure.

—End—

Configuring logging levels

Application

Use this procedure to configure the logging levels for these modules.

Action

Step	Action

At the IEMS workstation

1 Refer to "Launching IEMS Web Client" to launch the IEMS 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 the **Reset** button, if required, to reset to default values

8 You have completed this procedure.

—End—

Configuring user settings with Web Client

You can add users, modify user profiles, and delete users using Web Client. These operations are done using the User Admin tree in the Admin tab of the Web Client.

The Web Client allows the IEMS administrator to configure the following user setting tasks:

- "Adding a user using Web Client" (page 328)
- "Modifying a user profile using Web Client" (page 331)
- "Removing a user using Web Client" (page 334)

Navigating to the User Admin Tree in the Web Client

Application

Use this procedure to navigate to the User Admin tree in the Web Client.

Action

Step	Action
At the IEMS workstation	
1	Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111to launch the IEMS Client.
2	Select the **Admin** tab in the Web Client.
3	Select the **User Admin** node in the Module tree. You can expand the User Admin tree to find the sub-nodes Add User, Modify User Profile, and Delete User.
4	You have completed this procedure.

—End—

Adding a user using Web Client

Application

Use this procedure to add users.

The IEMS Web Client provides provision to add new users through the User Admin page. A new user can be added to any of the existing groups or to a newly defined group. The new user can also be provided access to selective IEMS operations.

Only a user of the secadm group can have access to all the IEMS operations.

Action

Step Action

At the Admin tab of IEMS Web Client

1 Refer to "Configuring user settings with Web Client" (page 327) to navigate to User Admin node of Web Client.

2 Click the **Add New User** node from the Module tree.

OR

Click **Add User** option from the User Admin page displayed on the right-side frame.

The Add User page is displayed.

3 Enter the unique user name for the user in the User Name field.

Refer to "User name compliance" (page 15)in "Adding a new user" (page 13)to set up the user name.

4 Enter a password in the Password field and confirm the password in the Confirm Password field.

The following password restrictions must be followed when setting or changing a user password through any security administration system integrated with the IEMS Security Server, including the IEMS itself.

- The password comprises a lowercase, an uppercase, and a numeric character. Special characters are also allowed and can be used if required.
- The user name cannot be longer than 8 characters.
- Passwords cannot be the same as a user name.

- Passwords expire after 2592000 seconds (30 days).
- You cannot change passwords more often than once in every 86400 seconds (1 day).

5 Select the group(s) to which the user must be a member from the Available Group Names list box. By default, a list of 33 groups are listed in the field

When adding APS users, the "mgcmtc" and "mgcadm" groups must be selected from the Group name(s) list.

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 Check the **Advanced User Details** check box.

The explanations of the fields to be filled under the **Advanced User Details** section is given in the following table:

Description of Advanced User Details properties

Field Name	Description
User ID	The user unique numerical ID for the machine (having Unix operating system). The ID is auto generated based on the range given in the NmsProcessessBE.conf file of /opt/nortel/iems/current/conf directory.
Primary Group	The unique numerical ID of the primary group to which the user belongs. You can select the group from the displayed list to which the added user is to be assigned.
Gecos	The user’s real name.
Expiry Date	The absolute date indicating the day from when the login can no longer be used. This value is derived from the sum of the number of days between the first day of the current year and the date the password was modified and the maximum number of days for which the password is valid. The value is then converted into a display date value.

Field Name	Description
Login Shell	The user initial shell program. It has the following two possible alternatives: "no-access" -- the user is disallowed from logging into the platform to obtain shell access. "restricted" -- by default, the user is permitted to log into the platform to obtain shell access. The shell rash is linked to a restricted shell, which is provided by the platform (if it is supported) or else it is linked to an unrestricted shell. Access to the unrestricted operations is available through a su (switch user) command.
Home Directory	The path name to the directory in which the user is initially positioned on logging in.
Min(days)	The minimum number of days required between the password changes. This insures that an expired password is not immediately reused by back-to-back requests to change the password. By default the value is 1.

8 Click the **Add User** button to add the user with the specified user details.

For Solaris and Linux OS machines, if a user name already exists in the machine register, then the same user cannot be added through the Security Administration GUI.

9 You have completed this procedure.

—End—

Modifying a user profile using Web Client

This section contains the following procedures:

- Modifying the user profile
- Changing user password in Web Client

The user of the *secadm* group of IEMS can change the password, enrollment of groups, and password and account expiry of existing users.

Modifying the user profile

Application

Use this procedure to modify the user's profile in Web Client.

Action

Step	Action
At the Admin tab of IEMS Web Client	
1	Refer to "Configuring user settings with Web Client" (page 327) to navigate to the User Admin node of Web Client.
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 **Modify User** 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, follow these steps: a. Enter the new password in the New Password field. b. Confirm the new password in the Confirm New Password field. *If the password is changed successfully, a* "Password has been successfully changed" message is displayed.

The password can be changed also using procedure mentioned in "Changing a user password in Web Client" (page 332).

6 Select the groups to which the user has to be enrolled in the Enrolled groups field using the **-->** and **<--** button.

The total number of groups that a user can belong to cannot exceed sixteen. The sixteen groups include groups created in IEMS and groups created at the SPFS or Solaris level.

7 Select the **Modify Password Expiration** box and provide the password expiry duration in days (if required).

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 Modify the fields provided under Advanced User Details section in the screen. For details on the fields, refer to "Description of Advanced User Details properties" (page 329).

9 Click the **Submit** button to update the changes.

10 You have completed this procedure.

—End—

Changing a user password in Web Client

Application

Use this procedure to change the password of current logged in user using Web Client.

Action

Step Action

At Admin tab of IEMS Web Client

1 Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.

2 Click the **Change Password** menu item provided at the top right side of the Web Client.

The Change Password page is displayed.

3 Enter the current password in the Current Password field.

4 Enter the new password in the New Password field.

5 Confirm the new password in the Confirm New Password field.

6 Click the **Submit** button.

If the password is changed successfully, "Password has been successfully changed" message is displayed.

7 You have completed this procedure.

—End—

Removing a user using Web Client

Application

Use this procedure to remove users.

The users who are not required have to be removed from IEMS. Removing a user removes the profile of the user.

Action

Step Action

At the Admin tab of IEMS Web Client

1 Refer to "Configuring user settings with Web Client" (page 327) to navigate to the User Admin node of Web Client.

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.

5 You have completed this procedure.

—End—

Carrier VoIP

IEMS Administration and Security

Publication: NN10336-611
Document status: Standard
Document version: 04.02
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to
http://www.nortel.com/documentfeedback

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.