Nortel Communication Server 1000

Enterprise Common Manager Fundamentals

NN43001-116

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Sourced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Revision history

May 2007
Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0

Contents

Procedures

New in this Release

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

The Enterprise Common Manager is a new NTP issued to support Communication Server 1000 Release 5.0.

Introduction

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

Purpose

This document contains information about the components, features, and benefits of the Enterprise Common Manager (ECM) framework. It describes ECM security management, including the various user account and identity configuration options and security polices for password thresholds. It discusses authorizations and permissions for built-in and custom role permission assignment that provide access control to the framework.

This document also provides information for the following ECM tasks:

- how to log on to the ECM and Linux Command Line Interface (CLI) in High Availability (HA) mode
- how to review and configure local account password policies
- how to manage and configure elements within ECM
- how to manage and configure users, roles, and permissions within ECM
- how to upgrade the primary or backup security service and member server
- how to configure system account passwords and Transparent Local Area Network (TLAN) and Embedded Local Area Network (ELAN) network interface IP addresses for the various server types within ECM

Navigation

- "Elements" (page 51)
- "Security" (page 77)
- "Tools" (page 117)
- "Upgrade" (page 123)
- "Backup and restore" (page 127)
- Appendix "Modify the IP addresses for installed servers" (page 131)
- Appendix "Linux root account Command Line Interface commands" (page 135)
- Appendix "Example of a least privilege algorithm" (page 139)
- Appendix "Example of role- and instance-based access control in CS 1000 systems" (page 141)
- Appendix "Red Hat passthrough end user license agreement" (page 145)

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or re-seller

If you purchased a service contract for your Nortel product from a distributor or authorized re-seller, contact the technical support staff for that distributor or re-seller.

Enterprise Common Manager overview

Contents

This chapter contains information on the following topics:

Introduction

The Enterprise Common Manager (ECM) provides users with an intuitive, common interface to manage and launch managed elements. ECM is a container that stores several system management elements in a single repository. Users need to sign in only once to access the elements. Users have access to all network system management elements in one framework. ECM eliminates the need for users to reauthenticate when they launch each system management application.

ECM provides framework-level security that simplifies security control for managed elements and system management applications. ECM manages secure access to Web applications and provides authentication and authorization with a single unified framework. ECM secures the delivery of essential identity and application information.

With ECM, administrators can control which users have access to specific managed elements. They can assign users to roles and map the permissions to those roles to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

With ECM, the integration of managed elements within a single container provides users with centralized security, user access control, simplified management tasks, improved workflow efficiency, convenience, and time-saving advantages.

Enterprise Common Manager components

The following elements are supported on the ECM framework for Release 5.0:

- Network Routing Service Manager: for the management of Network Routing Service data, including SIP proxy and H323 gateway
- The Communication Server 1000 (CS 1000) Element Manager: for the management of CS 1000 and Meridian 1 Release 5.0

Users access the framework through Microsoft Internet Explorer 6.02600 or later.

ECM runs on either an IBM 306 or an HP DL320 Commercial Off The Shelf (COTS) server. The following two deployment scenarios are available:

- Network Routing Service and Network Routing Service Manager installed with the ECM security framework on a dedicated COTS server
- CS 1000 Element Manager installed with the ECM security framework on a dedicated COTS server

ECM simultaneously supports up to 10 administrative users. Also, up to 1000 elements can be defined in one ECM server. Users can increase the number of elements by adding supplementary ECM servers. Regardless of how many ECM servers are installed, all elements within the same security domain appear in each ECM navigator.

For information about installing Linux and the ECM applications, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Benefits and features

The ECM framework is a generic system management software infrastructure that provides the following benefits and features:

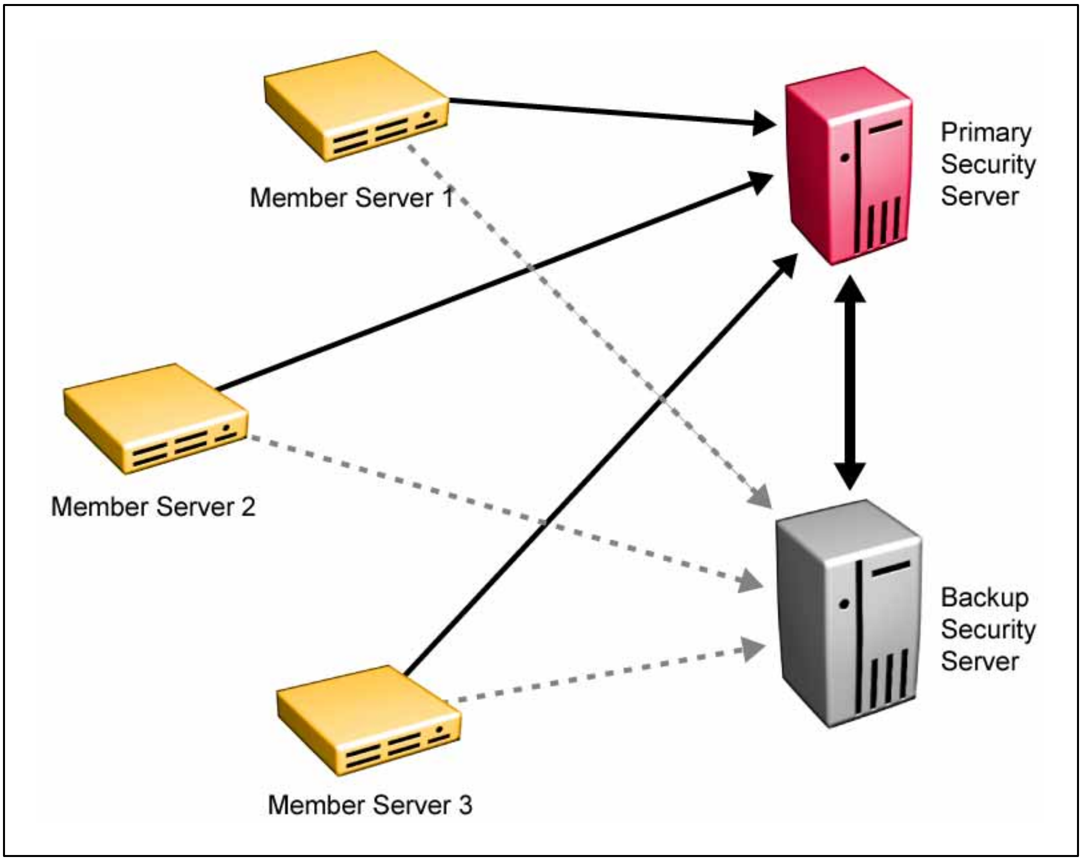
- central launch point for management facilities that oversee multiple network elements to manage the entire network
- common UI look and feel across all supported management facilities
- Web service interface where third-party developers can create applications to access ECM
- registry of the managed elements that launch the management applications
- security that provides Authentication, Authorization, and Auditing (AAA) for plug-in Web applications (elements) that reside within the ECM framework
- centralized security policy administration and enforcement
- private certificate authority and X.509 certificate management
- Single Sign On (SSO) and external Light Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS) authentication
- role- and instance-based access control
- local Simple Network Management Protocol (SNMP) management
- central point to manage users, passwords, and system access

Security domain

An ECM security domain is defined by the ECM primary security server. The ECM security domain is comprised of the ECM primary security server, the ECM backup security server, and associated member servers that contain the ECM framework and management applications. The primary security service or backup security service is not installed on a member server.

The primary security server must be the first server deployed in the security domain, as shown in Figure 1 "Security domain" (page 20).

Figure 1
Security domain



The primary security server is trusted by all servers in the security domain and is based on Secure Shell (SSH) public key authentication. All the servers in the security domain use the primary security server for authentication, authorization, and audit log storage.

When replication initializes between the backup security server and the primary security server, the backup security server is in a standby mode with the primary security server. When the primary security server is offline, servers in the security domain switch automatically to the backup security server for authentication, authorization, and audit log storage.

A management system can have one or more ECMs that are part of the same security domain. The security domain provides central authentication, authorization, and auditing for secure navigation between managed elements. All elements appear in a single navigator within the same security domain and run independently of ECM. The ECM framework provides the features and capabilities for all installed elements.

When a user logs on to ECM, the Elements Web page displays a list of the installed elements. A user need not reauthenticate to access a different element within ECM.

If firewalls exist between member servers, the backup security server, and the primary security server, users must open the following ports:

- ICMP port for ping
- TCP port 22 for SSH
- TCP port 80 for HTTP
- TCP port 443 for HTTPS
- TCP port 58080 for SAML
- TCP port 58081 for SAML secure mode
- TCP port 389 for LDAP
- TCP port 646 for LDAP
- TCP port 15080 for XMSG

Central launch point and common UI

The ECM security domain provides a central launch point for installed managed elements and bookmarked hyperlinks. A user can access a managed element when they log on to the ECM framework or through a direct Web link.

From the Elements Web page, a user accesses an element by performing one of the following:

- Clicking an element link.

  The selected element launches in the current browser window and replaces the ECM or element interface.

- Right-clicking the element and opening the element in a new browser window.
- Selecting the bookmarked element from the Favorites list in the browser window.

  The selected bookmarked element launches in the current window and replaces the ECM or element interface.

  To bookmark an element, right-click the element and select Add to favorites.

ECM provides a common UI that remains consistent between framework and element applications. The framework displays the links, specific to the selected element, in the left navigation pane. For example, if a user has selected NRS Manager from the element list, the NRS Manager replaces the ECM interface in the browser window and the NRS Manager navigation links appear in the left navigation pane.

Click the Common Manager link at the top of the left navigation pane to return to the ECM framework.

Certificate management

ECM uses certificate management: the X.509 certificate for Web Secure Sockets Layer (SSL) for secure communication between a Web browser and a Web server. In Release 5.0, certificates are used for the following:

- Web interfacing using SSL
- Session Initiation Protocol (SIP) signaling using Transport Layer Security (TLS)

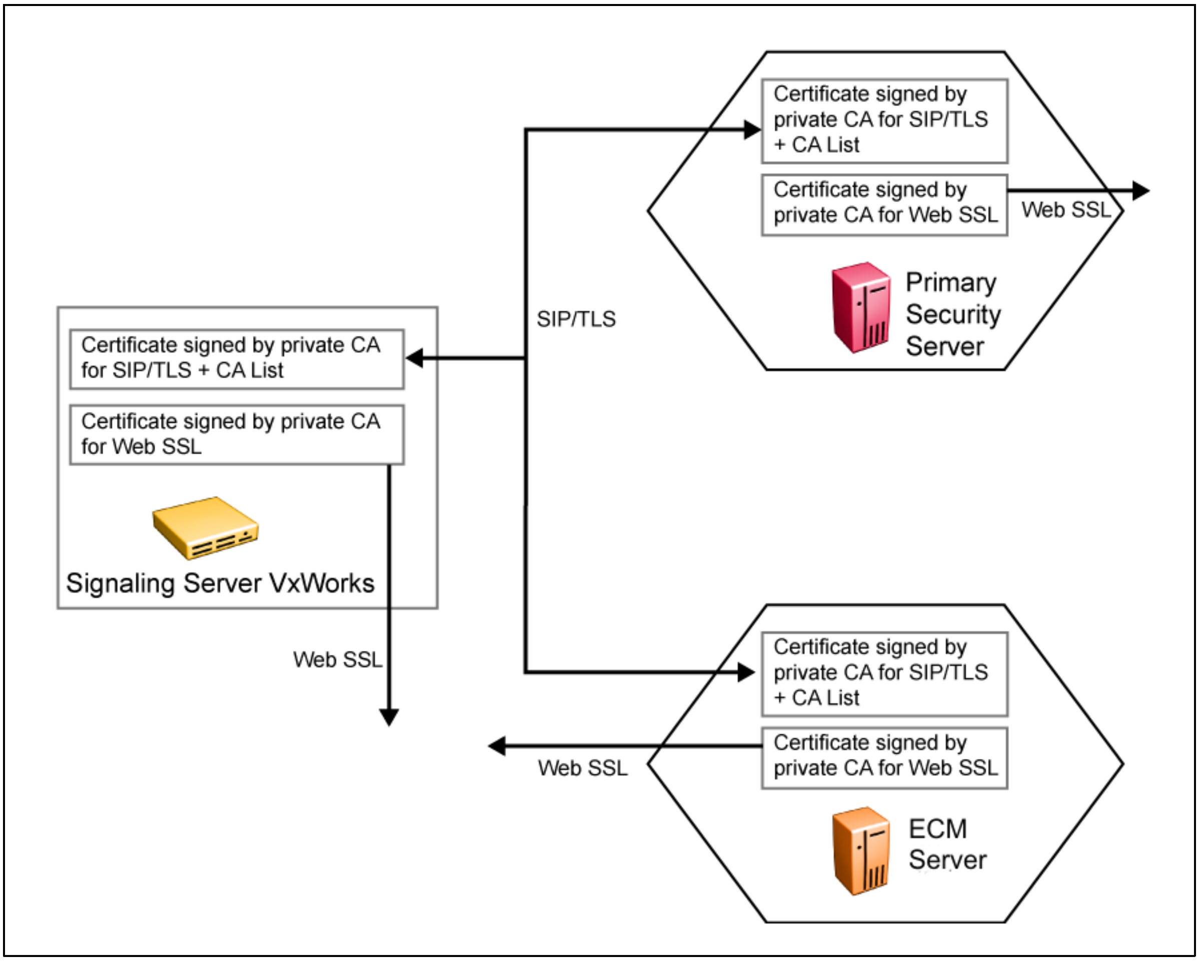
Within the ECM security domain, only one private Certificate Authority (CA) is used for CS 1000 to sign internally generated certificates. For certificate management in ECM, a private CA is configured only on the primary security server during installation. The private CA cannot be changed.

ATTENTION

With ECM, a private CA is always available on the primary security server. A user can choose to install the private CA to set up the trust on their system.

When the SIP TLS certificates, signed by the private CA, are distributed to the Network Routing Service or SIP Gateway, the private CA is automatically added to the trusted CA list of the Network Routing Service or SIP Gateway. Therefore, if all the Network Routing Service and SIP Gateway elements use certificates signed by the private CA, mutual authentication for SIP TLS is configured automatically between them. Similarly, users can install a certificate signed by the private CA on the server for Web SSL, as shown in Figure 2 "Certificates for SIP TLS and for Web SSL" (page 23).

Figure 2
Certificates for SIP TLS and for Web SSL


Certificate signed by private CA for SIP/TLS + CA List
Certificate signed by private CA for Web SSL
Web SSL
Primary Security Server
SIP/TLS
Certificate signed by private CA for SIP/TLS + CA List
Certificate signed by private CA for Web SSL
Signaling Server VxWorks
Web SSL
Certificate signed by private CA for SIP/TLS + CA List
Certificate signed by private CA for Web SSL
Web SSL
ECM Server

ATTENTION

Users must configure certificate management through the primary security server Web interface. Web interfaces from the other Linux servers cannot manage certificates.

Configuration for Secure Shell Trust of CA

SSH is used for the certificate management communication between SIP Proxy Servers (SPS). All SPS servers in the same security domain trust the primary security server where the private CA resides. The Rivest Shamir Adleman (RSA) public key of the primary security server is entered into the authorized key lists of all the servers.

Web SSL

A Web SSL certificate for ECM is installed when users install the application. The security administrator must configure the Web SSL certificate through the Certificates link of ECM on the primary security server.

For more information about certificate management, see *Security Management Fundamentals (NN43001-604)*.

Deployment

With ECM, the primary security service and backup security service are replicated. When one service is offline, the other service continues security service without affecting security service clients.

With ECM, there must be only one primary security service. The backup security service is optional. ECM can have one backup security service and one or more member servers for each ECM security service domain.

The ECM framework for a security domain is deployed in three distinct configurations.

- The primary security service consists of the following:
  - security service
  - security service client
  - certificate management module
  - Web server
- The backup security service consists of the following:
  - Linux host trust management module
  - security service
  - security service client
  - certificate management module
  - Web server

  The data from the primary security service is replicated to the backup security service. The backup security service provides security service if the primary security service fails.
- The member server consists of the following:
  - Linux host trust management module
  - security service client
  - certificate management module
  - Web server

The member server is the smallest footprint module. All member servers need IP connectivity to either the primary or backup security server. If this connectivity is down, users cannot log on to the member server Web pages.

ATTENTION
The certificate management module is the essential central security storage repository for the primary, backup, and member servers.

With ECM, two installation CDs provide six installation options.

The NRS CD provides the following three installation options:

- The Primary ECM Server (install NRS and the primary ECM security service)
- A Backup ECM Server (install NRS and a backup ECM security service)
- A Member Server (install NRS with ECM joining an existing secure network)

The Element Manager (MGMT) CD provides the following three installation options:

- The Primary ECM Server (install EM and the primary ECM security service)
- A Backup ECM Server (install EM and a backup ECM security service)
- A Member Server (install EM with ECM joining an existing secure network)

ATTENTION
The first Linux server must be installed with the primary security service. When the installation is complete for each installation option, the user must log on to ECM and add the element (Network Routing Service or Element Manager) that was installed on each server into the element table.

For more information about how to install the CS 1000 applications, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Audit logs

ECM supports the W3C extended log format. Logging is configured at the top-level of the framework and for each type of individual management system.

Log configuration

Table 1 "Types of log files in ECM" (page 26) describes the types of log files based on their content.

Table 1
Types of log files in ECM

Log file type	Description
***.alog**	Log activities in applications.
***.nlog**	Record activities in security provisioning changes and security enforcement.

The ECM framework logging feature records user activity, usage patterns, and authorization violations. The logs collect information such as denials, approvals, and code exceptions. The information is available only to security administrators.

Table 2 "Audit security logs available in the ECM security framework" (page 26) describes the two types of audit security logs stored in the ECM security framework.

Table 2
Audit security logs available in the ECM security framework

Types of audit security log	Description
Audit log for security administration	Record all operations that cause security configuration changes, such as the addition or deletion of a logged administrator.
Audit log for security enforcement	Record all operations that trigger security enforcement, such as logons and requests to access managed elements that are logged.

High Availability configuration

A script configures High Availability (HA) between the primary security service and the backup security service. The script must run from the primary security service Linux Command Line Interface (CLI) as root.

The primary and backup security services restart during the setup. A user must ensure that no user sessions are active before running the script.

Existing replication for the primary or backup security service is removed when the script runs.

Backup and restore

ECM supports backup and restore for the following data types:

- data from the certificate management module and the private CA module
- data from security service

For more information about backup and restore, see "Backup and restore" (page 127).

Security management

Contents

This chapter contains information on the following topics:

Overview

The Enterprise Common Manager (ECM) security framework enables element and service management applications to access a common application security infrastructure. The framework manages secure access to Web applications and provides security for Web interfaces and Web utilities.

The ECM security domain provides the central point for Authentication, Authorization, and Auditing (AAA); open, standards-based authentication; and policy-based authorization with a single, unified framework.

ECM provides access to various security features that enable system administrators to configure user and security rights within the application server. Security administrators can create new roles and assign default built-in roles to users within ECM. They can map permissions to a role for each user. Users see only what administrators authorize them to see based on their assigned roles and permissions.

With ECM, the authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of ECM.

Authentication

Authentication verifies the user’s login identity. With ECM, the user’s authentication is based on an assigned password.

Identity management

With identity management, security administrators can create, read, update, or delete user accounts.

Each user in a company has a unique digital identity. However, the unique identity can have different user accounts for different managed elements.

The ECM security framework supports the following account types:

- local account
- built-in account
- external account

Accounts

Local account

The ECM security framework maintains the data entry and password for a local user account and are stored in persistent storage.

Table 3 "Types of status for local user accounts" (page 30) lists the status types for a local user account.

Table 3
Types of status for local user accounts

Status Type	Description
Normal	An account with normal status has a valid password that is not expired.
Disabled	An account with disabled status cannot log on to ECM.
Logged in	An account with logged in status is currently accessing ECM.

Built-in account

ECM has one built-in account that is used by security administrators to log on to ECM after installation. The built-in account is assigned to built-in roles.

Table 4 "Supported built-in account" (page 30) describes the supported built-in account for ECM.

Table 4
Supported built-in account

Built-in account	Default password	Preassigned built-in roles	Description
admin	nortel12_Nortel	• SecurityAdministrator • ShellNortel • ShellPowerUser • ShellDebug	Use this account as the default account to log on to the ECM Web server after a new installation.

Built-in account	Default password	Preassigned built-in roles	Description
		• ShellAdvancedDebug	

ATTENTION

With the built-in admin account, security administrators can add, delete, and edit managed elements; but, they cannot directly access the management applications of the managed elements. Nortel recommends that security administrators create new accounts and assign roles to those accounts for access to the managed elements based on their specific security policy requirements.

External account

When an administrator is authenticated with external authentication with either Light Directory Access Protocol (LDAP) or Remote Authentication Dial In User Service (RADIUS), the external administrator account is added to ECM.

For Release 5.0, administrators can configure only one RADIUS or LDAP external authentication authority.

An external user has a shadow entry inside the persistent repository of the ECM security framework. The security framework uses the shadow entry to assign roles to the external user.

The password for an external account is stored in external authentication authorities. Users cannot initialize or change passwords for external users through ECM.

Central login

Central login authenticates all applications in a single security domain. Central login removes the need to manage multiple passwords on separate management applications within a Communication Server 1000 (CS 1000) system.

Central login is different from Single Sign On (SSO). Central login requires administrators to provide a logon name and password for each application. However, administrators use the same logon name and password for all applications inside the same security domain.

In a CS 1000 system, central login refers to the Command Line Interface (CLI) access for Linux hosts.

Security policies

With the ECM security framework, users can configure password and authentication settings.

Password aging policy enforcement

The password aging policy has the following time-based password thresholds that the security administrator can configure to number of days:

- minimum password age
- password expiration warning
- password expiration

Table 5 "Password aging policy thresholds" (page 32) describes what occurs when a user logs into ECM when the password aging policy thresholds expire.

Table 5
Password aging policy thresholds

Password threshold	What occurs when a threshold has expired
Minimum password duration	The user‘s new password is rejected when the current password has not reached the minimum password duration.
Password expiration warning	The user receives a password expiration warning when the password is about to expire and before the password expires.
Password expiration	The user is forced to change the password after the threshold for the password expires and before the threshold to disable the account. The password is locked until it is reset by the security administrator.

Password strength policy enforcement

The password strength policy requires a password to contain a minimum of six alphanumeric characters. In addition to letters and numeric digits, the password can contain special characters, such as an exclamation mark (!). The password can contain a combination of alphanumeric characters as defined by the security administrator.

If a password does not contain the required parameters for password requirements, the system rejects the password.

Password history policy enforcement

The password history policy verifies that a password is new. If a user enters a password previously used in the system, the password is rejected.

Password lockout policy enforcement

The lockout policy provides a limit for the number of attempts to access the ECM. The user is locked out of the framework when the specified number of login attempts is reached.

Users can change the password policies from the Password Policy Web page, as shown in Procedure 56 "Editing the password aging, history, strength, and lockout policies" (page 111).

Inactive session termination policy

The system suspends a user after 30 minutes of inactivity. A user must log on to ECM again when this occurs.

Login warning banner

ECM provides the text for the login warning banner that a security administrator can change, as shown in Procedure 57 "Editing the login warning banner" (page 115).

Authentication scheme policy

ECM supports up to three authentication authorities:

- local servers
- external RADIUS servers
- external LDAP servers (including Sun ONE or Microsoft active directory server)

The authentication servers policy controls the settings for the external LDAP and RADIUS servers.

Users can configure the authentication scheme, as shown in Procedure 53 "Editing the authentication scheme" (page 107).

Access control policies

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of ECM and its managed elements.

Authorization supports both Role Based Access Control (RBAC) and Instance Level Access Control (ILAC).

RBAC controls which users have access to protected resources based on user roles. Access rights are grouped by role name, and access to a managed element is restricted to users who are assigned the role name.

ILAC controls which users can apply an operation on a specific instance of a managed element, such as NRS Manager or Element Manager, based on the roles of the user and the permissions of the element granted to the roles. ILAC determines if the request is allowed or denied.

The ECM security framework uses the instance and RBAC data model. RBAC identifies the following five administrative elements:

- users

- roles
- permissions
- operations
- managed elements

With RBAC, administrators can customize user role assignments for each user within ECM. They can also map permissions to roles so that assigned users can perform only specific configurations on an element.

The ECM security framework implements RBAC with Access Control Lists (ACL). An ACL entry specifies which set of predefined actions a user with a certain role can perform on a managed element. For example, the role of nrsmAdmin can be granted administration access to a network routing service.

Table 6 "Features supported in the ECM security access control service" (page 34) describes the features supported in the ECM security framework access control service.

ATTENTION

Roles in CS 1000 are independent of ECM roles. Users must separately configure roles for CS 1000 management systems and for ECM.

Table 6
Features supported in the ECM security access control service

Features	Description
Centralized access control policy administration and review	Users provision, modify, and review user role and role permission assignments from a central point.
Centralized access control decision point	At runtime, RBAC denies or allows the current user to apply certain operations to a managed element from a central point.
Distributed access control policy enforcement	Implemented on each network element. Supports various systems with different access control enforcement policies for each type of system.
Multiple access control enforcement modules	Users access only Web pages they are authorized to see. If a user tries to access an unauthorized site, they receive an HTTP 403 Access Denied Error. Also, if an unauthorized user tries to directly access the business logic layer, for example, through Web service client, an Access Denied Exception message is sent to the user.

The least privilege algorithm in an authorization decision

With ECM, a user can have multiple assigned roles with access control entries on the same managed element. When a user attempts to access the managed element, the authorization decision is processed and the user is granted the permissions for the least privileged role. See, Appendix "Example of a least privilege algorithm" (page 139) for an example of how the least privilege algorithm is used within a company.

Built-in roles

Security administrators use built-in roles to manage user access control. Built-in roles control user permissions to various elements in ECM. Built-in roles are assigned to default permissions when a new element is added in ECM.

Table 7 "Built-in roles" (page 35) describes the built-in role permission assignment for the ECM security framework.

Table 7
Built-in roles

Built-in role types	Default role-permission assignment
SecurityAdministrator	The user has full access to users, roles, and security policies.
PowerUser	The user can perform operations, administration, and maintenance for elements within ECM.
Debugger	The user can access advanced debug utilities.
Patcher	The user can access software maintenance functions.
NrsmMonitor	The user has read-only access to Network Routing Service elements.
CS1000_Level1	The user has full access to overlays and customers.
ShellNortel	The user has full access to software install, upgrade, and maintenance commands from the Linux CLI.
ShellPowerUser	The user can access provisioning commands for applications from the Linux CLI.
ShellDebug	The user can access debugging commands from the Linux CLI.
ShellAdvanceDebug	The user can access advanced level debugging commands from the Linux CLI.
LinuxDebug	The user can access operating system level debugging.

When administrators add a new element to ECM, the built-in roles are assigned default permissions to the element. Built-in roles are read-only. A user cannot modify or delete built-in roles.

Table 8 "Built-in role permission assignments for CS 1000 elements" (page 36) shows the built-in role permission assignments for CS 1000 elements.

Table 8
Built-in role permission assignments for CS 1000 elements

Built-in role name	**Permissions assigned to the built-in role for a CS 1000 element**
PowerUser	Give the user all of the permissions for CS 1000.
CS1000_Level1	Give the user full access to overlays and customers.
Patcher	Give the user access to the following: • PDT1 and PDT2 • Overlays 117, 135, 22, 43 (used for CPP system) required to launch EM

Table 9 "Built-in role permission assignments for the Network Routing Service" (page 36) shows the built-in role permission assignments for the Network Routing Service.

Table 9
Built-in role permission assignments for the Network Routing Service

Built-in role name	**Permissions assigned to the built-in role for the Network Routing Service**
PowerUser	The user can perform operations, administration, and maintenance on the Network Routing Service.
NrsmMonitor	The user has read-only access to Network Routing Service elements.

For an example of role- and instance-based access control, role permission assignments, and user role assignments for users in ECM, see Appendix "Example of role- and instance-based access control in CS 1000 systems" (page 141).

Command Line Interface commands

Contents

This chapter contains the following topics:

Perform the procedures in this chapter from the Command Line Interface (CLI). For each CLI command, log on to the CLI with a root account and run the CLI command script.

Configure system account passwords

System accounts provide internal communication between applications in the Enterprise Common Manager (ECM). When the primary security server is installed, users must change the default password. The default password strength policy requires a password to contain a minimum of 12 characters. It must also contain at least one number, 0 through 9, one special character, such as an exclamation mark (!), and one uppercase and one lowercase character.

When a user installs the backup and member servers, the current system password is sent from the primary security server to isclients on all servers in the security domain.

System account passwords never expire. Use a change_syspassword.sh script to change the system password in the security domain when the installation is complete. Users must run the change_syspasswd.sh script from the primary security server. The new password automatically synchronizes to the backup security server and member server.

Change the system account password for the security domain from the primary security server

When the primary security server is installed, users must provide a new password for system accounts.

Use the steps in Procedure 1 "Changing the system account password from the primary security service" (page 38) to change the system account from the primary security service.

Run the change_syspasswd script only when all Linux servers in `/root/.ssh/know_hosts` are online.

Procedure 1

Changing the system account password from the primary security service

Step	Action
1	Log on to the primary security server CLI.
2	At the prompt, enter **`su`** to switch to superuser mode.
3	At the prompt, enter the root password.
4	Run the **`/opt/nortel/isclient/change_syspasswd.sh`** script.
5	Enter a new password, and then confirm the new password. The password is sent to the isclient on the primary security server, the backup security server, and the member server.

—End—

Send system account password changes to the isclient on the primary, backup, and member servers

Use the steps in Procedure 2 "Sending system account password changes to the isclient on the primary, backup, and member servers" (page 38) to send the system account password changes to the isclient on the primary security server, the backup security server, and member server.

Use the following procedure if the servers are offline when the system account password is changed from the primary security service.

Procedure 2

Sending system account password changes to the isclient on the primary, backup, and member servers

Step	Action
1	Log on to the primary security server.

2 At the prompt, enter **`su`** to switch to superuser mode.

3 At the prompt, enter the root password.

4 Run the **`/opt/nortel/isclient/change_syspasswd.sh-sync`** script.

Users need not provide the new password.

The current system account password is sent to the isclient security server, the backup security server, and the member server.

—End—

Reset a user password from the CLI

A security administrator can reset a password account from the ECM Web interface. However, when a security administrator password is expired or forgotten, the password must be reset from the CLI.

Use the steps in Procedure 3 "Resetting a user password from the CLI" (page 39) to reset the password from the CLI.

Procedure 3

Resetting a user password from the CLI

Step **Action**

1 Log on to the Linux CLI using an SSH or serial port console.

2 At the prompt, enter **`su`** to switch to superuser mode.

3 At the prompt, enter the root password.

4 To reset the password, run the **`/opt/nortel/applications/security/current_isclient/bin/is_passwd.sh -server write`** script.

5 Enter the user name to change.

6 Enter the new password.

7 Confirm the new password.

—End—

Configure the High Availability from the primary security server

Use the steps in Procedure 4 "Configuring the HA from the primary security server" (page 40) to configure the High Availability (HA) from the primary security server.

Procedure 4
Configuring the HA from the primary security server

Step	Action
1	Log on to the primary security server.
2	At the prompt, enter **`su`** to switch to superuser mode.
3	At the prompt, enter the root password.
4	To configure the HA, run the **`/opt/nortel/isclient/setup_ssha.sh config`** script.
5	To clear the configuration of the HA, run the **`/opt/nortel/isclient/setup_ssha.sh deconfig`** script.

—End—

Backup and restore security data

For information about how to back up and restore the ECM security data, see "Backup and restore " (page 127).

For the complete list of Linux root account CLI commands, including debug commands, see Appendix "Linux root account CLI commands" (page 135).

Use the Enterprise Common Manager

Contents

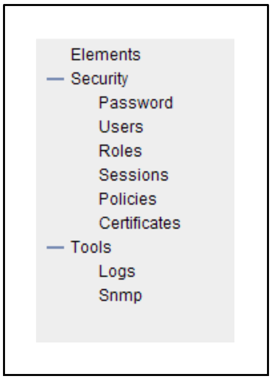
This chapter contains the following topics:

This chapter provides a description of the links available in the Enterprise Common Manager (ECM) navigation pane. It also provides information to configure the ECM default password and to log on and log off of ECM.

Enterprise Common Manager navigator links

The ECM framework navigator is located on the left side of the browser window, as shown in Figure 3 "ECM Navigator" (page 42).

Figure 3
ECM Navigator



Links in the navigation pane are structured as follows:

- **Elements**
- **Security**
  - Password
  - Users
  - Roles
  - Sessions
  - Policies
  - Certificates
- **Tools**
  - Logs
  - SNMP

Elements

The Elements section contains links to the managed elements (application plug-ins and bookmarks). From this Web page users can add a new element or edit or delete an existing element.

Security

The Security section contains the following links to manage security features in ECM.

- Password: Use this link to view the status for a password or to change the password.
- Users: Use this link to view administrative users, to add a new administrative user, or to disable or delete an existing administrative user.

- Roles: Use this link to view user role assignments or to add or delete a role name. Users can also view the element permissions and description assigned to a role.
- Sessions: The sessions link displays all users who are currently logged on and displays the session time for each user.
- Policies: Use this link to configure the authentication scheme and authentication servers, establish password policies, and edit security settings.
- Certificates: Use this link to configure the information for certificate configuration status.

Tools

The Tools section contains links for ECM logging information and SNMP configuration.

- Logs: Use this link to view management activity logs for all servers in the ECM framework. Users can open log files directly or download log files for offline analysis.
- SNMP: Use this link to view the current status for Simple Network Management Protocol (SNMP) configuration. Users can edit, enable, or disable existing SNMP information or configure SNMP community strings for access to Management Information Base (MIB) and SNMP trap destinations for error reporting.

Change the ECM default password

Use the steps in Procedure 5 "Changing the ECM default password" (page 43) to launch Enterprise Common Manager (ECM), log on for the first time, and to change the default password.

When the ECM installation is complete, for the first-time log on, users must use the default user name and password to log on and then they must change the default password. Users must also follow the default password strength policy.

Default password strength policy

The default password strength policy requires a password to contain a minimum of eight characters. It must also contain at least one number, 0 through 9, one special character, such as an exclamation mark (!), and one uppercase and one lowercase character.

Procedure 5

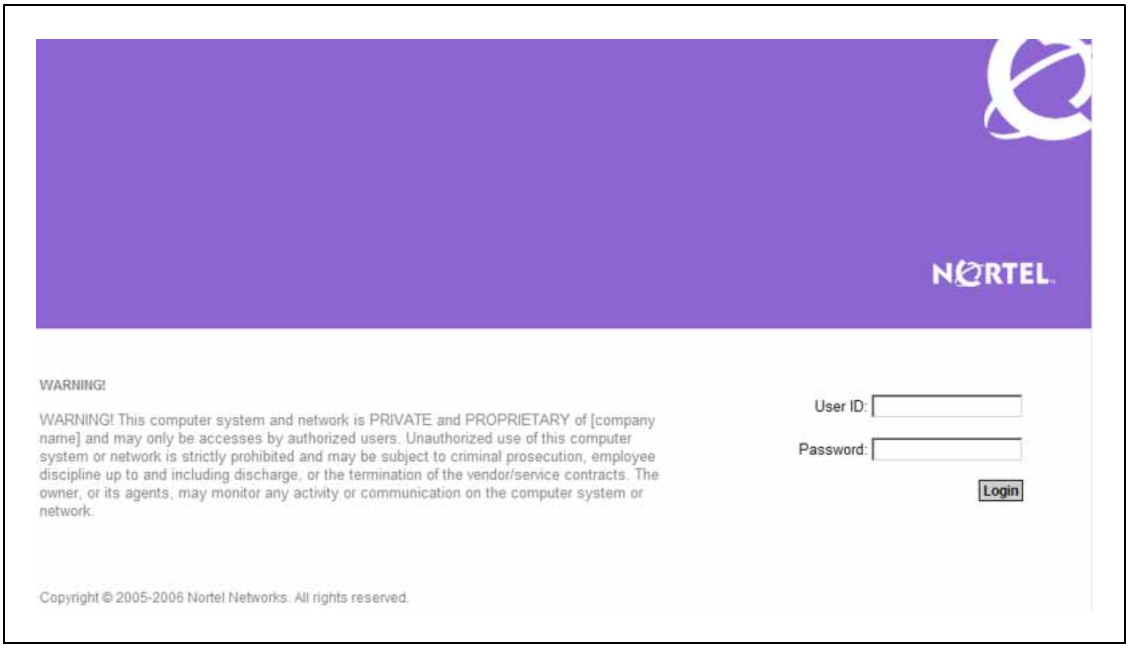
Changing the ECM default password

Step	Action
1	Open the Web browser.

2 Enter the ECM framework IP address or domain name in the **Address** bar and press **Enter**.

The ECM framework appears with the **Login** Web page, as shown in Figure 4 "Login Web page" (page 44).

Figure 4
Login Web page



WARNING!

WARNING! This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accesses by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

Copyright © 2005-2006 Nortel Networks. All rights reserved.

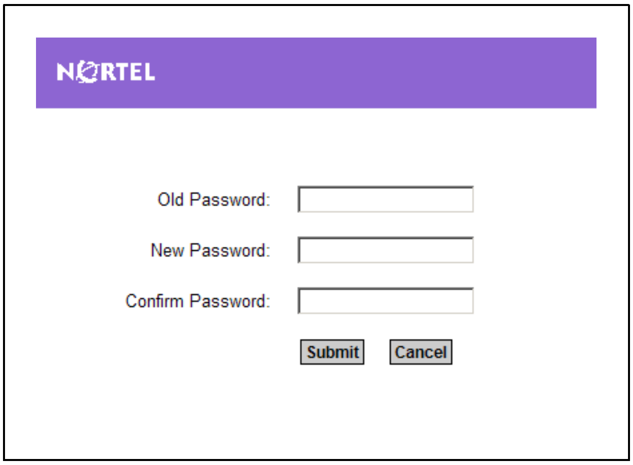
3 In the **User ID** field, type `admin`.

> **ATTENTION**
> User names in ECM are not case-sensitive. However, Linux-based user names that are independent of ECM are case-sensitive.

4 In the **Password** field, type `nortel12_Nortel`.

The **Nortel** Web page appears to change the password, as shown in Figure 5 "Nortel Web page" (page 45).

Figure 5
Nortel Web page



Old Password:

New Password:

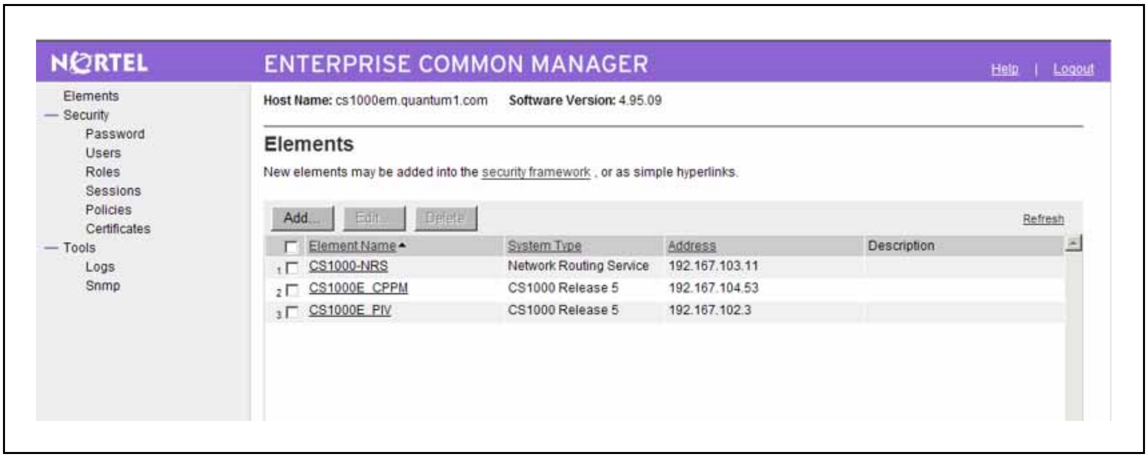
Confirm Password:

5 From the **Nortel** Web page, perform the following tasks:

- In the **Old Password** field, type the old password.
- In the **New Password** field, type a new password.
- In the **Confirm Password** field, type the new password.
- Click **Submit**.

The default navigation Web page for ECM appears, as shown in Figure 6 "Enterprise Common Manager navigation Web page" (page 45).

Figure 6
Enterprise Common Manager navigation Web page



Host Name: cs1000em.quantum1.com **Software Version:** 4.95.09

Elements

New elements may be added into the security framework , or as simple hyperlinks.

	□	Element Name ▲	System Type	Address	Description
1	□	CS1000-NRS	Network Routing Service	192.167.103.11	
2	□	CS1000E_CPPM	CS1000 Release 5	192.167.104.53	
3	□	CS1000E_PIV	CS1000 Release 5	192.167.102.3	

—End—

Log on options in ECM

Use the following procedures to log on to ECM using various options such as High Availability (HA) mode, Single Sign On (SSO), web authorization (webauth) servlet, and external authentication.

Log on to ECM in HA mode when the primary security service is offline

Use the steps in Procedure 6 "Logging on to ECM in high availability mode when the primary security service is offline" (page 46) to log on to ECM in HA mode when the primary security service is offline.

By default, the log on is provided by the primary security service. When the primary security service is offline, use the local login Web page to switch to the backup security service.

Procedure 6

Logging on to ECM in HA mode when the primary security service is offline

Step **Action**

1 In a Web browser, type `https://fqdnOfServer` to log on to ECM.

The Web browser shows the message that the Web page cannot be displayed because the primary security service is offline.

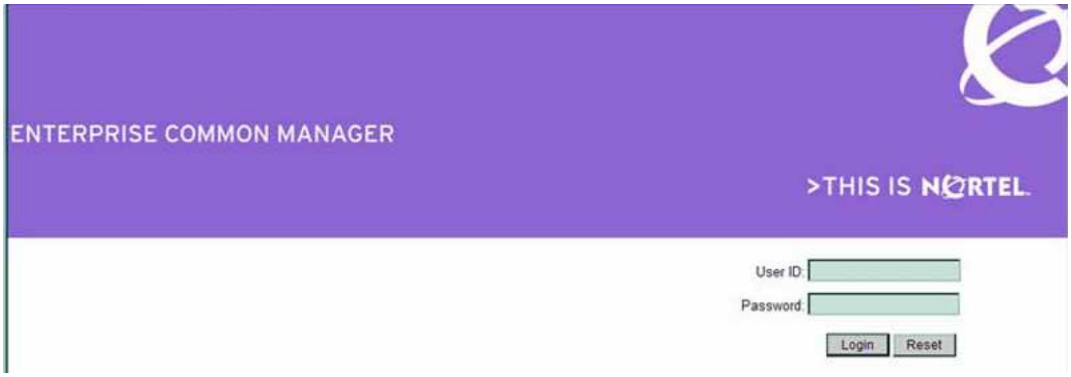
2 Type `https://fqdnOfServer/localLogin` in the **Address bar** to Log on to ECM.

The local login Web page appears, as shown in Figure 7 "Local login Web page" (page 46).

ATTENTION

Passwords that must be changed at login cannot be used in the local login page. The local login page does not support warning banner, expired password change, and reset scenarios.

Figure 7
Local login Web page



3 Enter a valid user ID and password combination, and click **Login**.

The ECM navigation Web page appears.

The Policies link is available only when a user logs on to the primary security server.

—End—

Log on to Linux CLI in HA mode when the primary security service is offline

To log on to Linux CLI in HA mode when the primary security service is offline, use an ECM account through Secure Shell (SSH).

Log on with Web authorization servlet from the backup security server

Use the steps in Procedure 7 "Logging on to the backup security server with webauth servelet" (page 47) to log on to the backup security service with the webauth servlet.

Procedure 7

Logging on to the backup security server with webauth servlet

Step Action

1 In a Web browser, type `https://fqdnOfBackupSecurity-Server:58081/webauth/webauthservlet` to log on to ECM.

The login page appears.

2 Enter a valid user name and password combination, and click **Login**.

An empty Web page appears.

3 Type `https://fqdnOfBackupSecurityServer or https://fqdnOfMemberServer` in the **Address** bar to Log on to ECM.

The ECM navigation Web page appears.

The Policy link is available only when a user logs on to the primary security server.

—End—

Log on with Single Sign On for Web-based applications using the Fully Qualified Domain Name

Use the steps in Procedure 8 "Logging on with SSO between Web applications within the same ECM" (page 48) to log on to the system with Single Sign On (SSO) between applications and the ECM framework. All Web applications must be inside the same DNS domain to support SSO.

Procedure 8
Logging on with SSO between Web applications within the same ECM

Step	Action
1	Enter the Fully Qualified Domain Name (FQDN) in the **Address** bar of the browser window, and press **Enter**. The application **Login** Web page appears.
2	Type a valid user name and password combination.
3	Click **Login**. The application Web page appears.
4	Enter the FQDN or click the link of an element in the same Web browser window. When an element is installed on the same ECM, the selected element Web page appears without the user having to reauthenticate.

—End—

Log on with SSO between Web applications in multiple ECMs

Use the steps in Procedure 9 "Logging on with SSO between Web applications in multiple ECMs" (page 48) to log on to ECM with SSO between Web applications in multiple ECMs.

SSO support for Web access is available when the Fully Qualified Domain Name (FQDN) name is used and when all Web applications are inside the same DNS domain.

The two IP addresses use the same Sun Access Manager as the primary security service.

Procedure 9
Logging on with SSO between Web applications in multiple ECMs

Step	Action
1	Enter the ECM IP address in the **Address** bar of the Web browser, and press **Enter**.

2 Enter a valid user name and password combination.

3 From the **Elements** page, click an element link.

When the element management URL is located on a different ECM, the user is redirected to the Web page of the selected element without having to reauthenticate.

—End—

SSO for Web-based applications using FQDN without DNS infrastructure

The FQDN uses an IP address with DNS. To use SSO for Web access without DNS infrastructure, users must enter the FQDN in `\WINNT\system32\drivers\etc\hosts` in the Web browser Window Operating System (OS).

If users use a non-Windows OS for Web clients, refer to the OS document to configure the corresponding setup.

The IP address to FQDN mapping in the `\WINNT\system32\drivers\etc\hosts` must be the same as the IP address in the Linux hosts `/etc/hosts` where ECM is installed.

ATTENTION

A user name and password that is not in the local user database is denied access to the Linux host CLI.

Log off options

Table 10 "Log off options in ECM" (page 49) describes how to log off from the ECM framework and how to log off globally for elements within the same or different ECM system.

Table 10
Log off options in ECM

Log off method	Action	Result
Log off from the ECM framework	Click Logout at the top right corner of the window.	A Web page appears confirming the logout was successful.

Log off method	Action	Result
Log off globally	Click Logout at the top right corner of the window and then, from the same browser window, type the URL of another Web application running within ECM.	The user is redirected to the ECM login Web page.
Log off globally for Web applications in a different ECM	Click Logout at the top right corner of the window and then, from the same browser window, type the URL of a Web application that runs within a different ECM.	The user is redirected to the ECM login Web page.

Elements

Contents

This chapter contains the following topics:

Manage elements

Elements is the default Web page that opens when the Enterprise Common Manager (ECM) is launched. When the user clicks the Elements link in the Security branch of the ECM navigator, the Elements Web page appears. From the Elements Web page, users can view, add, edit, delete, or launch elements within the ECM framework. Use the procedures in this chapter to manage the elements in ECM.

The ECM framework manages the following elements:

- Bookmark
- CS 1000 Release 5
- Network Routing Service
- SIP Gateway

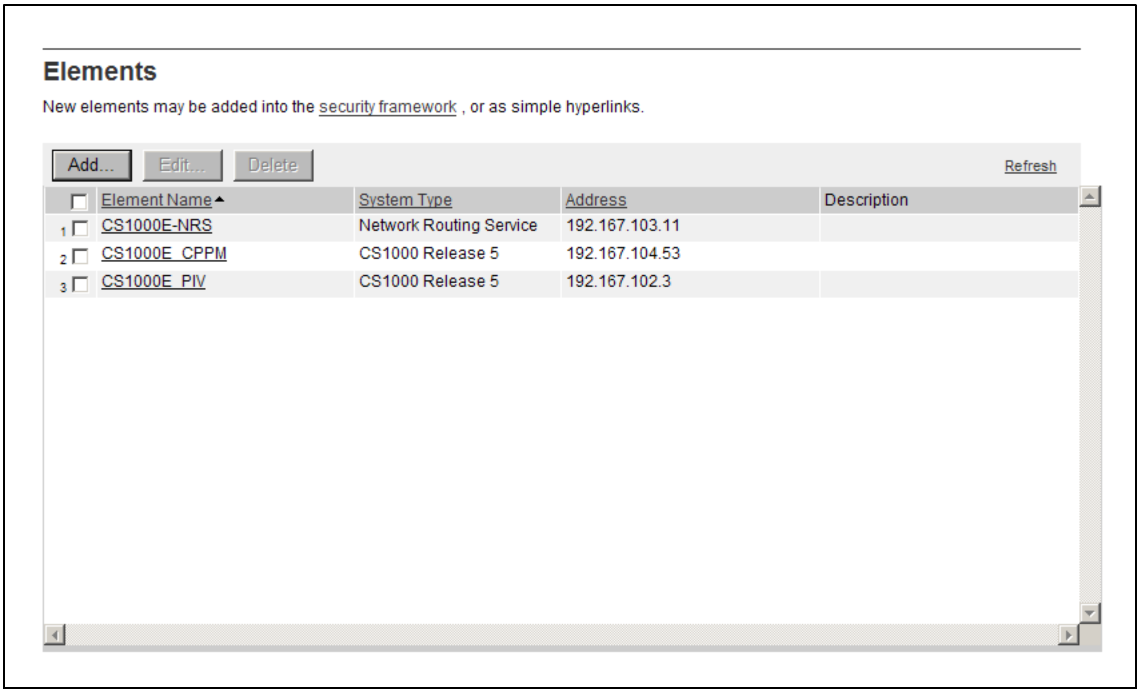
Launch a managed element

Use the steps in Procedure 10 "Launching a management application for an element and bookmarking the application" (page 52) to launch the management application for a selected element in the current or a new Web browser and to bookmark a management application for an element.

Procedure 10
Launching a managed element

Step	Action
1	Log on to ECM.
2	From the navigation pane, click **Elements**. The **Elements** Web page is the default Web page that appears when ECM is opened, as shown in Figure 8 "Elements Web page" (page 52).

Figure 8
Elements Web page



Elements

New elements may be added into the security framework , or as simple hyperlinks.

	□	Element Name▲	System Type	Address	Description
1	□	CS1000E-NRS	Network Routing Service	192.167.103.11	
2	□	CS1000E_CPPM	CS1000 Release 5	192.167.104.53	
3	□	CS1000E_PIV	CS1000 Release 5	192.167.102.3	

Step	Action
3	In the **Element Name** column, click the element name link. The management application for the element appears in the same Web browser window. To launch an element in a new browser window, right-click the element and select **Open in new window**.

To bookmark management applications for an element in a new Web browser window, right-click the element link and select **Add to favorites**.

—End—

Add elements

The following procedures provide information to add a Network Routing Service, CS 1000 Release 5, SIP Gateway, and bookmark element in ECM.

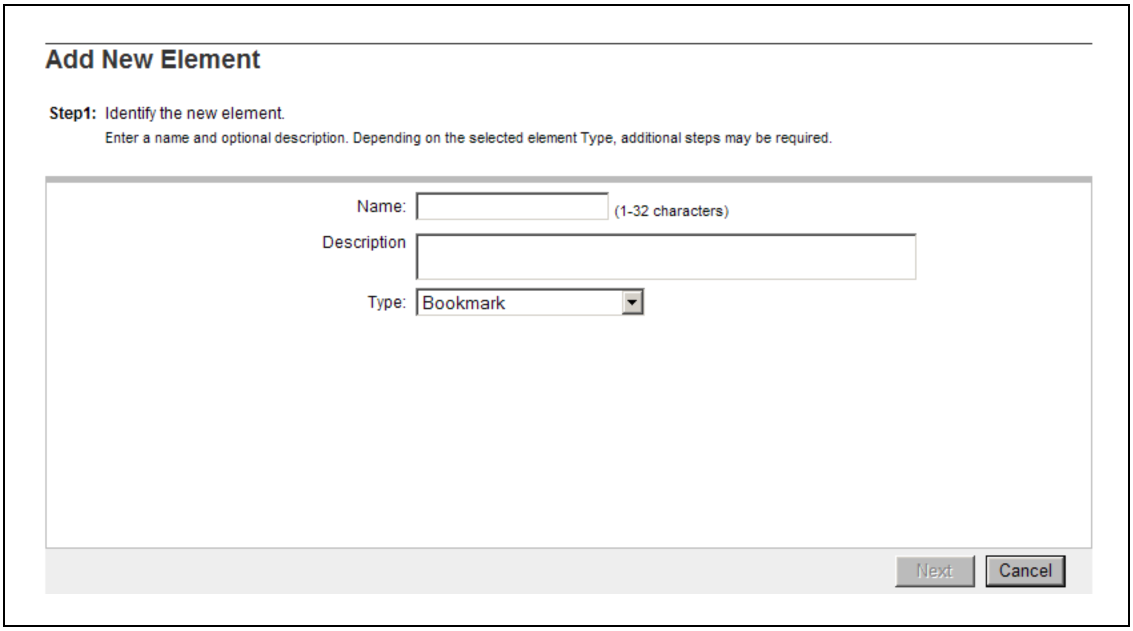
Add a bookmark

Use the steps in Procedure 11 "Adding a bookmark" (page 53) to add an external hyperlink element in ECM.

Procedure 11
Adding a bookmark

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	From the **Elements** Web page, click **Add**. The **Add New Element Step 1** page appears, as shown in Figure 9 "Add New Element Step 1 Web page" (page 54).

Figure 9
Add New Element Step 1 Web page



Add New Element

Step1: Identify the new element.
Enter a name and optional description. Depending on the selected element Type, additional steps may be required.

Name: (1-32 characters)

Description

Type: Bookmark

4 In the **Name** field, type the element name.

> **ATTENTION**
> The name must be from 1 to 32 characters.

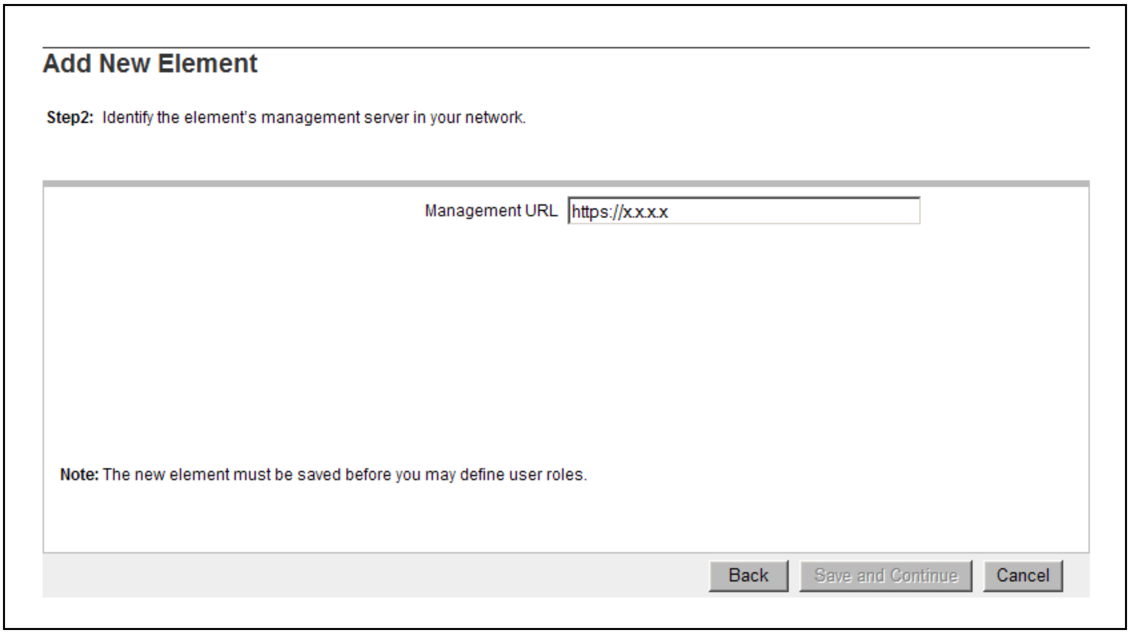
5 In the optional **Description** field, type a description if required.

6 Select **Bookmark**.

7 Click **Next**.

The **Add New Element Step 2** Web page appears for the Bookmark element, as shown in Figure 10 "Add New Element Step 2 for Bookmark Web page" (page 55).

Figure 10
Add New Element Step 2 for Bookmark Web page



Add New Element

Step2: Identify the element's management server in your network.

Management URL: https://x.x.x.x

Note: The new element must be saved before you may define user roles.

8 In the **Management URL** field, type the URL for the bookmark element.

9 Click **Save and Continue**.

—End—

Add a CS 1000 Release 5 element

Use the steps in Procedure 12 "Adding a CS 1000 Release 5 element" (page 55) to add a CS 1000 Release 5 element in ECM.

Procedure 12
Adding a CS 1000 Release 5 element

Step Action

1 Log on to ECM as a security administrator.

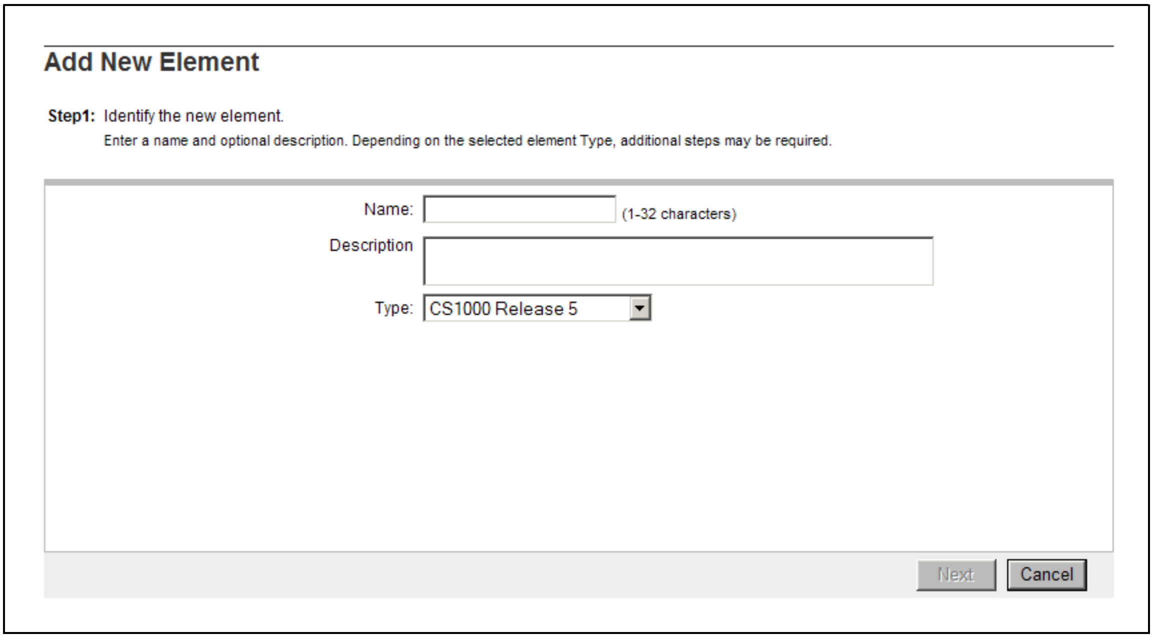
2 From the navigation pane, click **Elements**.

The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).

3 From the **Elements** Web page, click **Add**.

The **Add New Element Step 1** page appears, as shown in Figure 11 "Add New Element Step 1 Web page" (page 56).

Figure 11
Add New Element Step 1 Web page



Add New Element

Step1: Identify the new element.

Enter a name and optional description. Depending on the selected element Type, additional steps may be required.

Name: (1-32 characters)

Description

Type: CS1000 Release 5

4 In the **Name** field, type the element name.

> **ATTENTION**
> The name must be from 1 to 32 characters. Nortel recommends that users make this the host name.

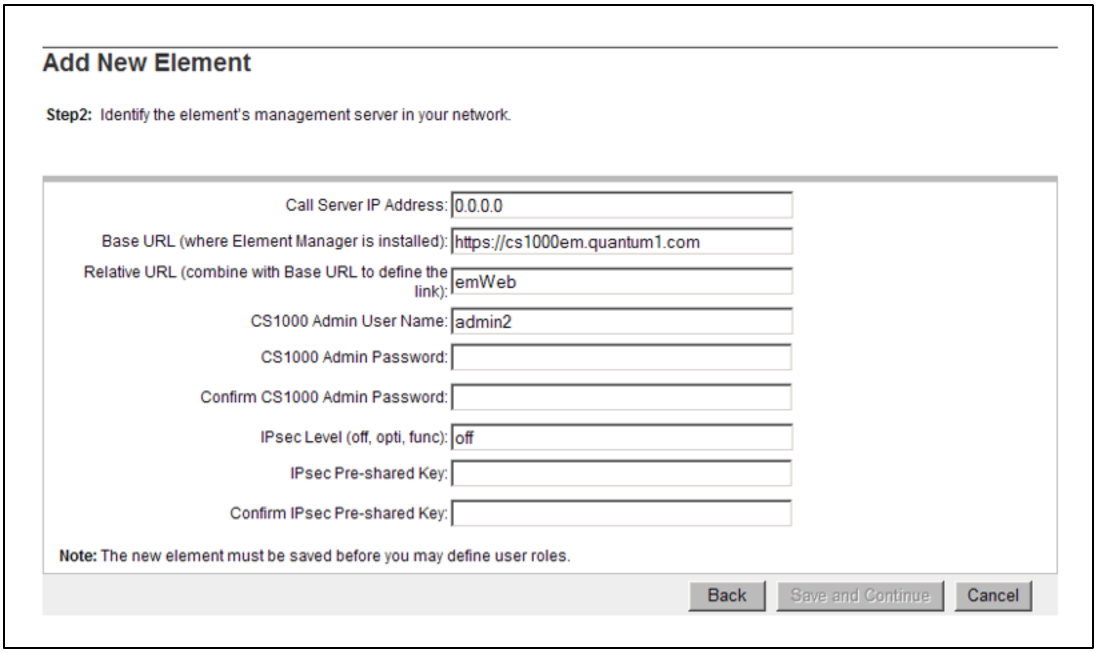
5 In the optional **Description** field, type a description if desired.

6 From the **Type** list, select **CS1000 Release 5**.

7 Click **Next**.

8 The **Add New Element Step 2** page appears, as shown in Figure 12 "Add New Element Step 2 for CS 1000 Release 5" (page 57).

Figure 12
Add New Element Step 2 for CS 1000 Release 5



Add New Element

Step2: Identify the element's management server in your network.

Call Server IP Address: 0.0.0.0

Base URL (where Element Manager is installed): https://cs1000em.quantum1.com

Relative URL (combine with Base URL to define the link): emWeb

CS1000 Admin User Name: admin2

CS1000 Admin Password:

Confirm CS1000 Admin Password:

IPsec Level (off, opti, func): off

IPsec Pre-shared Key:

Confirm IPsec Pre-shared Key:

Note: The new element must be saved before you may define user roles.

9 In the **Call Server IP Address** field, type the call server IP address of the CS 1000 system.

10 Review the default value for the **Base URL** property.

The default value is where Element Manager is installed.

11 Review the default value of the **Relative URL** property.

The default value for CS 1000 is `emWeb`. The default value should not be changed.

12 In the **CS1000 Admin User Name** field, type the user name.

The user name must be an existing name that the CS 1000 system uses.

> **ATTENTION**
>
> The privilege level of the user name you enter for CS 1000 must match the privilege level of the user role you use when operating ECM. Therefore:
>
> - If the ECM user has the Power User role, enter information for an admin2 account that is configured on the CS 1000 system.
> - If the ECM user has any other role, enter information for an admin1, admin2, or LAPW account that is configured on the CS 1000 system.

13 In the **CS1000 Admin Password** field, type the password.

ATTENTION

The password must be the same as the CS 1000 admin user password on the CS 1000 system.

14 In the **Confirm CS1000 Admin Password** field, type the password.

15 In the **IPsec Level (off, opti, func)** field, type the IPsec level.

The choices for IPsec level are as follows:

- off: IPsec is off
- opti: optimal level that secures XMSG and PbxLink messaging
- func: functional level that uses IPsec to protect packets that travel between Linux and Node elements including the Call Server

ATTENTION

Ensure the IPsec level on ECM is the same as the IPsec level on the CS 1000 system. Failing to do so can cause some or all traffic to be blocked.

An error message appears and traffic is blocked when the IPsec levels for CS 1000 and ECM do not match. Do not configure the IPsec with mismatched levels for CS 1000 and ECM, as shown in Table 11 "Mismatched IPsec levels on CS 1000 and ECM" (page 58).

Table 11
Mismatched IPsec levels on CS 1000 and ECM

IPsec level on CS 1000	IPsec level on ECM	Result
FULL	OFF	Traffic is blocked.
FUNC	OFF	Traffic is blocked.
OFF	FUNC	Traffic is blocked.
OFF	OPTI	Traffic is blocked.
FULL	OPTI	Traffic is blocked.
FUNC	OPTI	Traffic is blocked.
OPTI	FUNC	Traffic is blocked.

16 In the **IPsec Pre-shared Key** field, type the IPsec preshared key.

The preshared key is only required when IPsec is enabled with the opti or func level.

ATTENTION

The preshared key must contain between 16 and 32 characters and must be the same as the preshared key entered on the call server.

The preshared key must not contain any of the following special characters:

~ * \ ’ @ [] #

17 In the **Confirm IPsec Pre-shared Key** field, type the IPsec preshared key.

18 Click **Save and Continue**.

—End—

If the ECM manages more than one CS 1000 system, users must add the preshared key information for each Call Server to ECM before users can launch Element Manager to communicate with the Call Server.

When IPsec parameters are changed on the Call Server, the ECM security administrator must make the same parameter changes for IPsec on the ECM server.

Change of preshared key

When the preshared key is changed on the Call Server, the ECM security administrator must make the same change in ECM for preshared key, as shown in Procedure 16 "Editing the properties of a CS 1000 Release 5 element" (page 66). The IPsec configuration takes effect when a user launches Element Manager.

New node element

When a new node element is added, the ECM security administrator must run the Linux shell script to manually enable the link between the ECM server and the new node element.

The following scripts are located in the /opt/nortel/ipsec directory. To run the scripts, users must perform the following tasks:

- Log on to the primary security server Command Line Interface (CLI) with account nortel.
- At the prompt, enter su to switch to superuser mode.
- At the prompt, enter the root password.

To manually enable the link between the ECM server and the new node element, run **`addIPsecTarget.sh <IP address> <pre-sharedkey> <IPsec security level>`**.

On the new element, the ECM security administrator must add the IP address of the Call Server and ECM as the target for IPsec.

- To add the new target, run **`isecNewTarget`**.
- To enable the new target, run **`isecEnlTarget`**.
- To view the new target added in the IP Sec profile, run **`isecProfileShow`**.

The ECM security administrator must also add the new element IP address as a target for the Call Server through the LD 117 command and run **`new isecTar <address of the new element>`**.

The ECM security administrator can now add this new element in the node in Element Manager and complete the save and transfer of the IP Telephony configuration files to all the node elements.

Deleted node element

When a node element is deleted, the ECM security administrator must run the following Linux shell script to manually disable the link and remove the IP table entry of the node element on the Linux server.

```
removeIPsecTarget.sh <IP address>
```

Use the steps in to disable the link and remove the IP table entry for a node element on the ECM server.

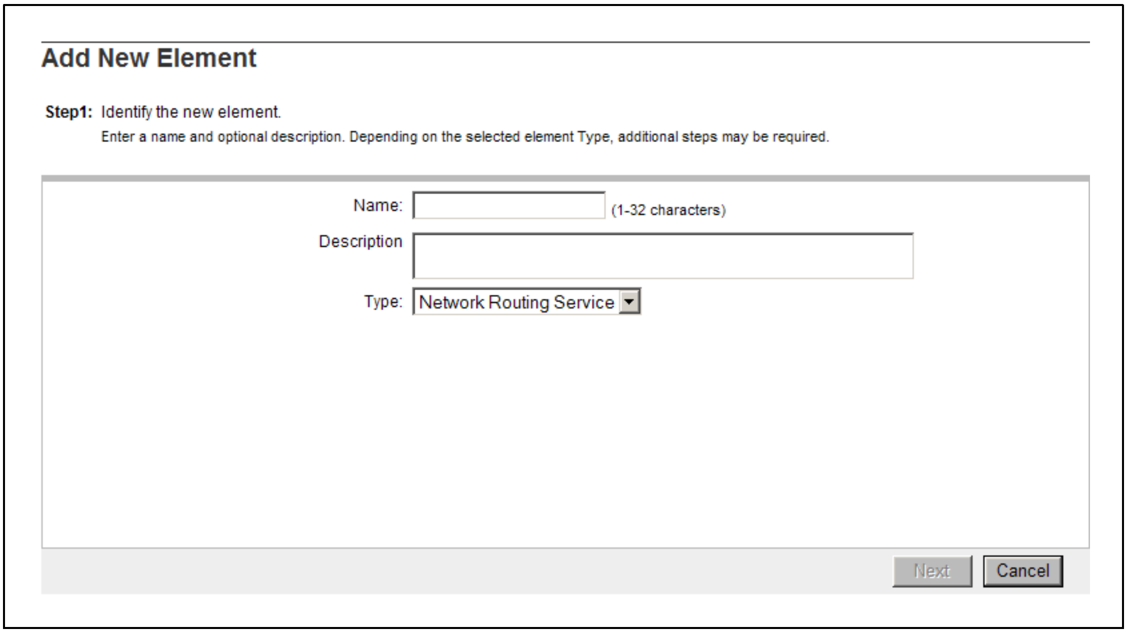
Add a Network Routing Service element

Use the steps in Procedure 13 "Adding a Network Routing Service element" (page 60) to add a Network Routing Service element in ECM.

Procedure 13
Adding a Network Routing Service element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	From the **Elements** Web page, click **Add**. The **Add New Element Step 1** page appears, as shown in Figure 13 "Add New Element Step 1 Web page" (page 61).

Figure 13
Add New Element Step 1 Web page



Add New Element

Step1: Identify the new element.

Enter a name and optional description. Depending on the selected element Type, additional steps may be required.

Name: (1-32 characters)

Description

Type: Network Routing Service

4 In the **Name** field, type the element name.

> **ATTENTION**
> The name must be from 1 to 32 characters. Nortel recommends that users make this the host name.

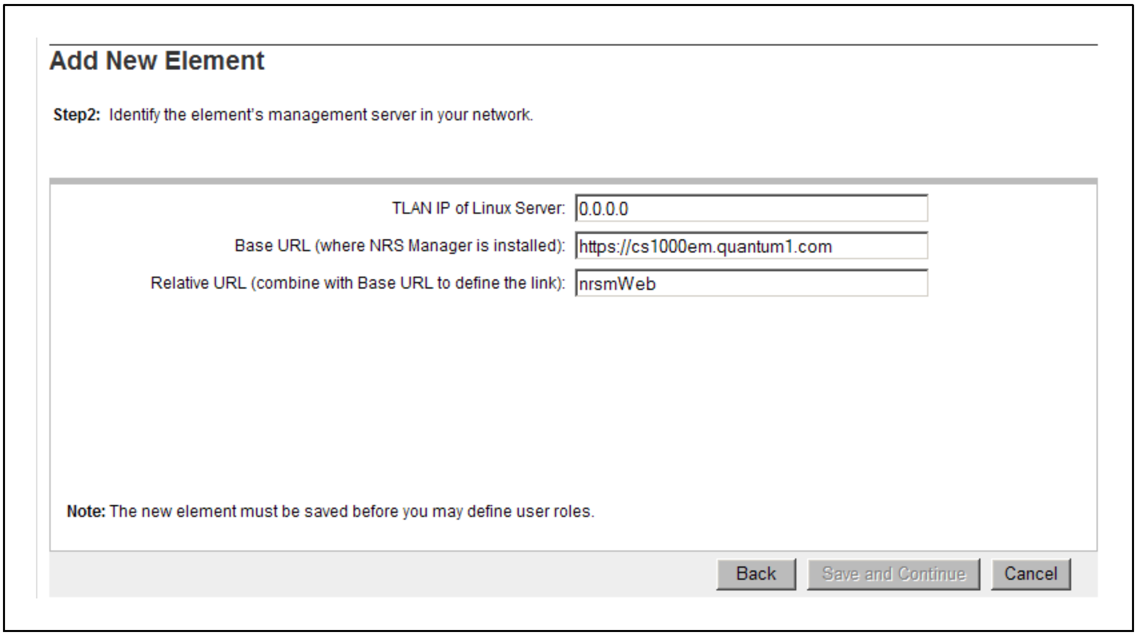
5 In the optional **Description** field, type a description if desired.

6 From the **Type** list, select **Network Routing Service**.

7 Click **Next**.

The **Add New Element Step 2** page appears, as shown in Figure 14 "Add New Element Step 2 for Network Routing Service" (page 62).

Figure 14
Add New Element Step 2 for Network Routing Service



Add New Element

Step2: Identify the element's management server in your network.

TLAN IP of Linux Server: 0.0.0.0

Base URL (where NRS Manager is installed): https://cs1000em.quantum1.com

Relative URL (combine with Base URL to define the link): nrsmWeb

Note: The new element must be saved before you may define user roles.

8 In the **TLAN IP of Linux Server** field, type the TLAN IP address or the Fully Qualified Domain Name of the Linux host where the Network Routing Service is installed.

9 Review the default value for the **Base URL** property.

> **ATTENTION**
> The default value of the Base URL is resolved from the currently accessed ECM Web server. If the Network Routing Service is installed on a different ECM Web server, change the Base URL as necessary.

10 Review the default value of the **Relative URL** property.

The default value for Relative URL for the Network Routing Service is `nrsmWeb`.

11 Click **Save and Continue**.

—End—

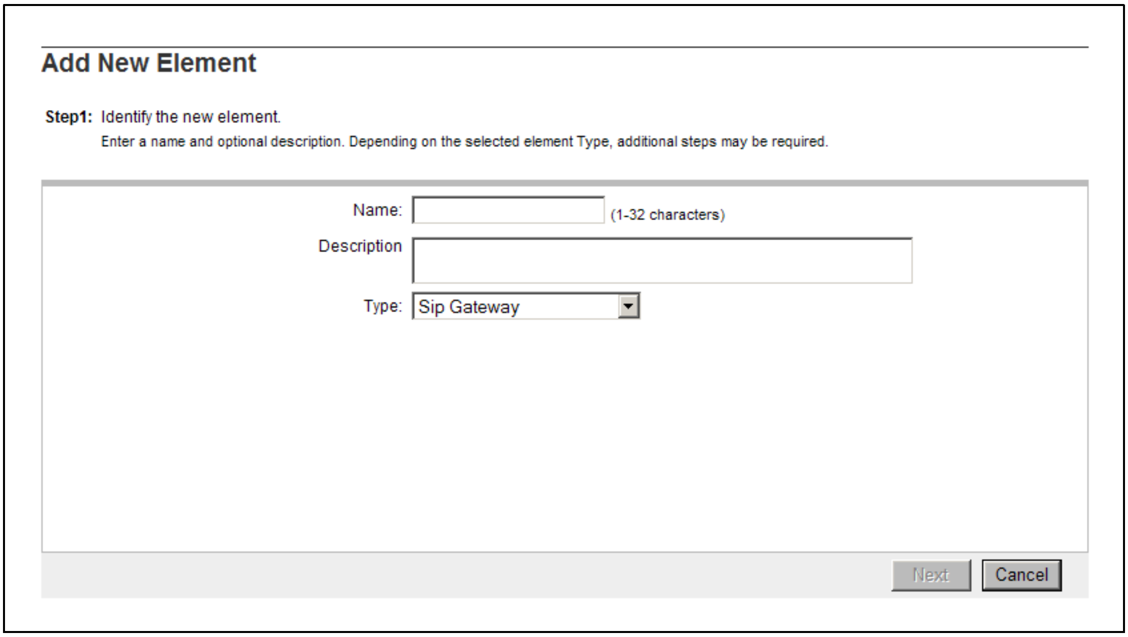
Add a SIP Gateway element

Use the steps in Procedure 14 "Adding a SIP Gateway element" (page 63) to add a VxWorks-based signaling server element in ECM.

Procedure 14
Adding a SIP Gateway element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	From the **Elements** Web page, click **Add**. The **Add New Element Step 1** page appears, as shown in Figure 15 "Add New Element Step 1 Web" (page 63).

Figure 15
Add New Element Step 1 Web



Add New Element

Step1: Identify the new element.
Enter a name and optional description. Depending on the selected element Type, additional steps may be required.

Name: (1-32 characters)

Description

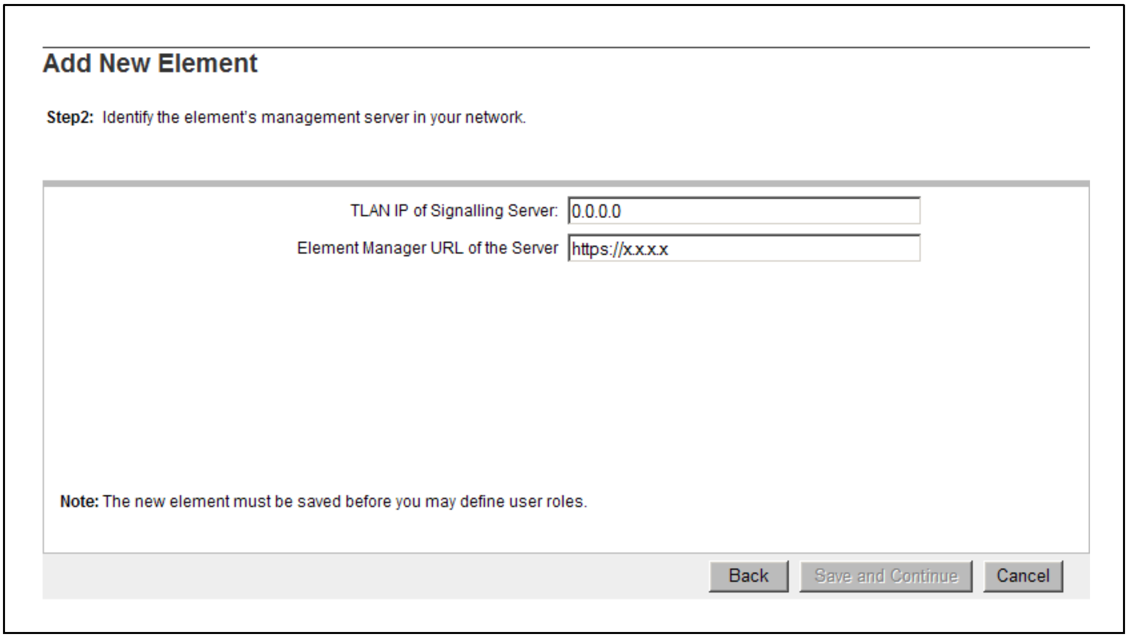
Type: Sip Gateway

4	In the **Name** field, type the element name.

> **ATTENTION**
> The name must be from 1 to 32 characters. Nortel recommends that users make this the host name.

5	In the optional **Description** field, type a description if desired.
6	From the **Type** list, select **SIP Gateway**. The **Add New Element Step 2** Web page for SIP Gateway appears, as shown in Figure 16 "Add New Element Step 2 Web page for SIP Gateway" (page 64)

Figure 16
Add New Element Step 2 Web page for SIP Gateway



Add New Element

Step2: Identify the element's management server in your network.

TLAN IP of Signalling Server: 0.0.0.0

Element Manager URL of the Server https://x.x.x.x

Note: The new element must be saved before you may define user roles.

7 Click **Next**.

8 In the **TLAN IP of Signalling Server** field, type the TLAN IP address for the signaling server.

9 In the **Element Manager URL of the Server** field, type the Element Manager URL for the signaling server.

10 Click **Save and Continue**.

—End—

Edit element properties

Use the procedures in this section to edit the properties of a bookmark, CS 1000 Release 5, Network Routing Service, or SIP Gateway element installed in ECM.

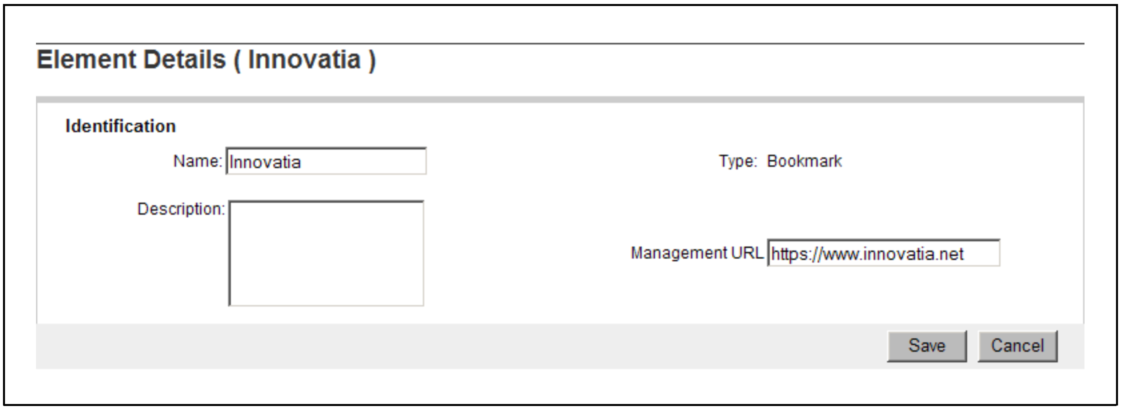
Edit the properties of a bookmark element

Use the steps in Procedure 15 "Editing the properties of a bookmark element" (page 65) to edit the properties of a bookmark element in ECM.

Procedure 15
Editing the properties of a bookmark element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	From the **Elements** Web page, select the check box beside the bookmark element to edit, and click **Edit**.
4	The **Element Details** Web page for the selected bookmark element appears, as shown in Figure 17 "Element Details Web page for a bookmark element" (page 65).

Figure 17
Element Details Web page for a bookmark element



Element Details (Innovatia)

Identification

Name: Innovatia

Type: Bookmark

Description:

Management URL https://www.innovatia.net

Step	Action
5	From the **Identification** section, edit the following fields as required: • Name • Description • Management URL
6	Click **Save**.

—End—

Edit the properties for a CS 1000 Release 5 element

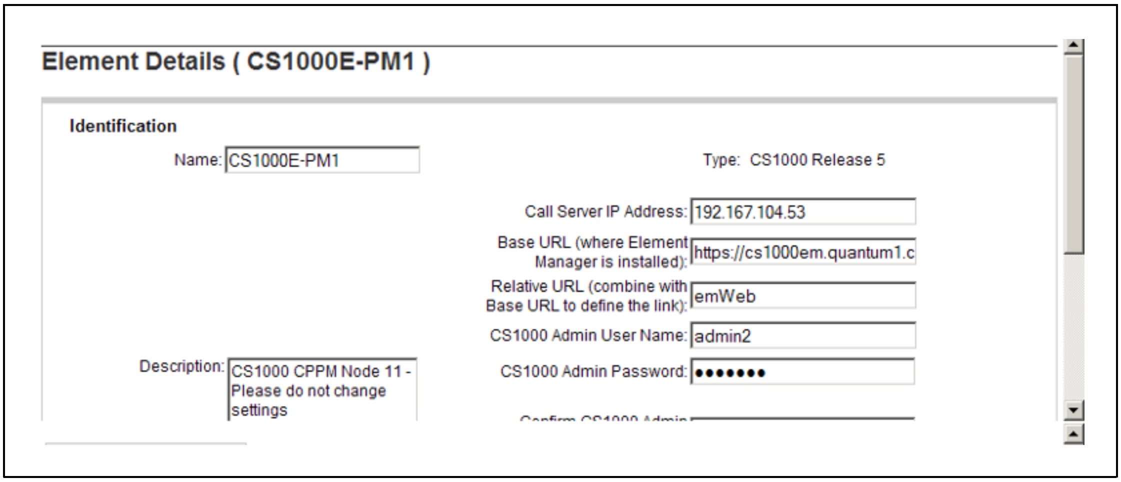
Use the steps in Procedure 16 "Editing the properties of a CS 1000 Release 5 element" (page 66) to edit the properties of a CS 1000 Release 5 element.

Procedure 16

Editing the properties of a CS 1000 Release 5 element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	From the **Elements** Web page, select the check box beside the CS1000 Release 5 element to edit, and click **Edit**.
4	The **Element Details** Web page appears, as shown in Figure 18 "Element Details Web page for a CS 1000 Release 5 element" (page 66).

Figure 18
Element Details Web page for a CS 1000 Release 5 element



Element Details (CS1000E-PM1)

Identification

Name: CS1000E-PM1

Type: CS1000 Release 5

Call Server IP Address: 192.167.104.53

Base URL (where Element Manager is installed): https://cs1000em.quantum1.c

Relative URL (combine with Base URL to define the link): emWeb

CS1000 Admin User Name: admin2

Description: CS1000 CPPM Node 11 - Please do not change settings

CS1000 Admin Password: •••••••

Step	Action
5	From the **Identification** section, edit the following fields as required:

- Name
- Description
- Call Server IP Address
- Base URL (where Element Manager is installed)
- Relative URL (combine with Base URL to define the link)
- CS1000 Admin User Name
- CS1000 Admin Password
- Confirm CS1000 Admin Password
- IPsec Level (off, opti, func)

- IPsec Pre-shared Key
- Confirm IPsec Pre-shared Key

6 Click **Save**.

—End—

Edit the properties for a Network Routing Service element

Use the steps in Procedure 18 "Editing the properties of a Network Routing Service element" (page 68) to edit the properties of a Network Routing Service element.

Procedure 17

Editing the properties of a Network Routing Service element

Step Action

1 Log on to ECM as a security administrator.

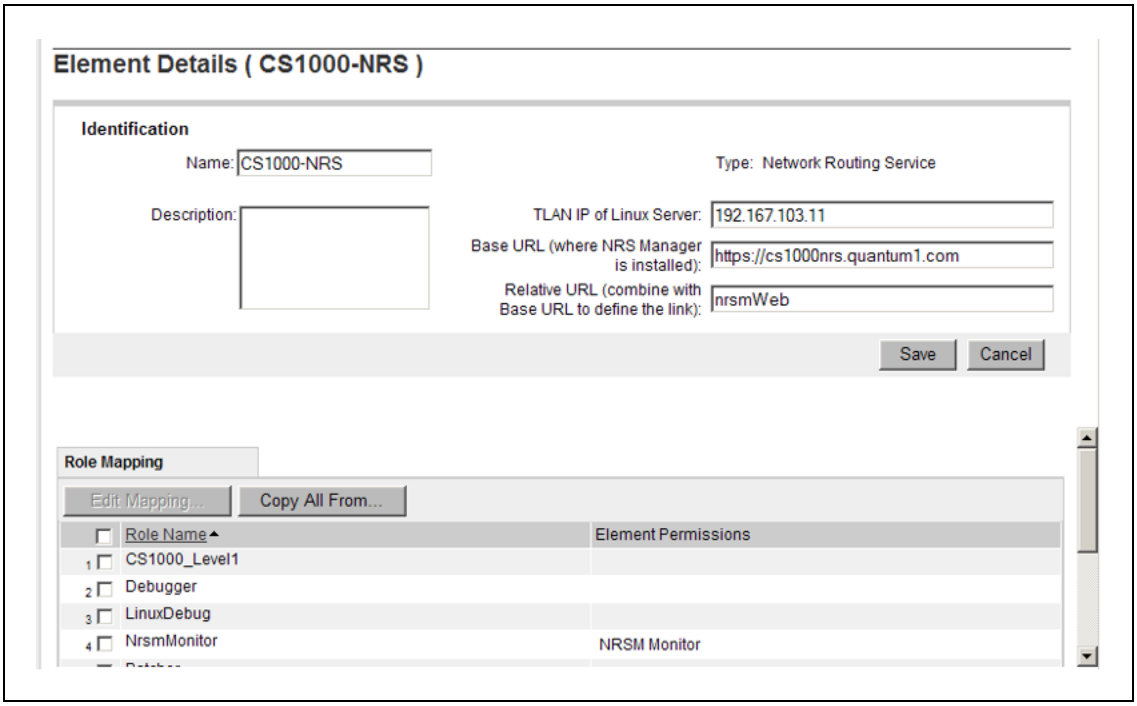
2 From the navigation pane, click **Elements**.

The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).

3 From the **Elements** Web page, select the check box beside the element to edit, and click **Edit**.

4 The **Element Details** Web page appears, as shown in Figure 19 "Element Details Web page for a Network Routing Service element" (page 68).

Figure 19
Element Details Web page for a Network Routing Service element



Element Details (CS1000-NRS)

Identification

Name: CS1000-NRS

Type: Network Routing Service

Description:

TLAN IP of Linux Server: 192.167.103.11

Base URL (where NRS Manager is installed): https://cs1000nrs.quantum1.com

Relative URL (combine with Base URL to define the link): nrsmWeb

Role Mapping

	□ Role Name ▲	Element Permissions
1	□ CS1000_Level1	
2	□ Debugger	
3	□ LinuxDebug	
4	□ NrsmMonitor	NRSM Monitor

5 From the **Identification** section, edit the following fields as required:

- Name
- Description
- TLAN IP of Linux Server
- Base URL (where NRS Manager is installed)
- Relative URL (combine with Base URL to define the link)

6 Click **Save**.

—End—

Edit the properties for a SIP Gateway element

Use the steps in Procedure 18 "Editing the properties of a SIP Gateway element" (page 68) to edit the properties of a SIP Gateway element.

Procedure 18
Editing the properties of a SIP Gateway element

Step	Action
1	Log on to ECM as a security administrator.

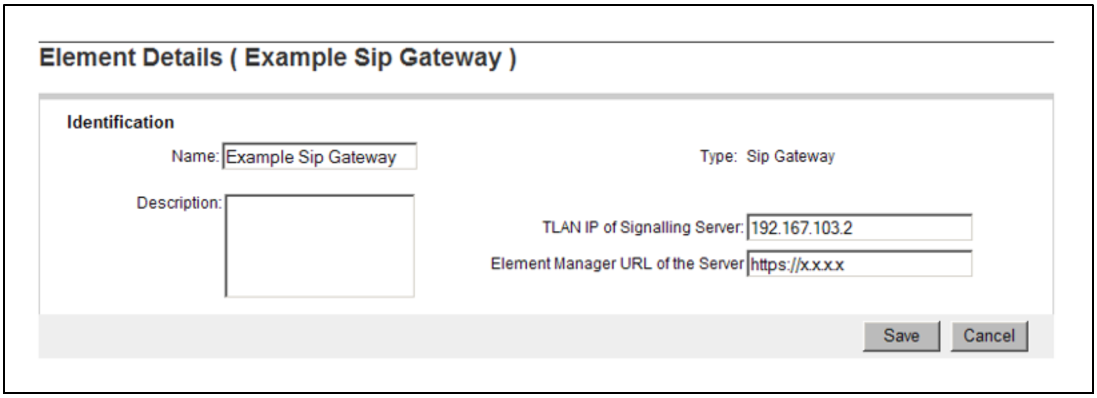
2 From the navigation pane, click **Elements**.

The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).

3 From the **Elements** Web page, select the check box beside the element to edit, and click **Edit**.

4 The **Element Details** Web page appears, as shown in Figure 20 "Element Details Web page for a SIP Gateway element" (page 69).

Figure 20
Element Details Web page for a SIP Gateway element



Element Details (Example Sip Gateway)

Identification

Name: Example Sip Gateway

Type: Sip Gateway

Description:

TLAN IP of Signalling Server: 192.167.103.2

Element Manager URL of the Server: https://x.x.x.x

5 From the **Identification** section, edit the following fields as required:

- Name
- Description
- TLAN IP of Linux Server
- Element Manager URL of the Server

6 Click **Save**.

—End—

Delete selected elements

Use the steps Procedure 19 "Deleting selected elements" (page 69) to delete elements that ECM no longer requires.

Procedure 19
Deleting selected elements

Step	Action
1	Log on to ECM as a security administrator.

2 From the navigation pane, click **Elements**.

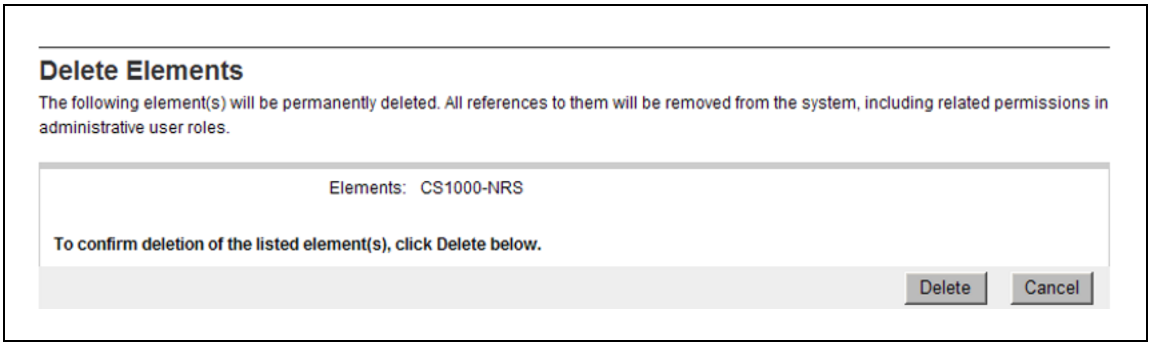
The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).

3 From the **Elements** Web page, select the check box beside one or more elements.

4 Click **Delete**.

The **Delete Elements** Web page appears, as shown in Figure 21 "Delete Elements Web page" (page 70).

Figure 21
Delete Elements Web page



Delete Elements

The following element(s) will be permanently deleted. All references to them will be removed from the system, including related permissions in administrative user roles.

Elements: CS1000-NRS

To confirm deletion of the listed element(s), click Delete below.

5 Click **Delete** to proceed with the deletion or **Cancel** to cancel the deletion.

—End—

ATTENTION

Accessing management applications of a deleted element

ECM maintains an in-memory cache for all elements accessed from the current Web server. When a user deletes an element, the in-memory cache still contains the information for the element. However, all permissions on an element are denied after the user deletes the element.

Edit element permissions to existing user roles for new elements

Use these procedures to edit the element role mapping using the Edit Mapping and Copy All From options for a new element in ECM.

Edit element role mapping with Edit Mapping

Use the steps in Procedure 20 "Editing element role mapping with Edit Mapping for a new element" (page 71) to map the permissions supported for a new CS 1000 Release 5, Network Routing Service, or SIP Gateway element to existing user roles with Edit Mapping.

Procedure 20
Editing element role mapping with Edit Mapping for a new element

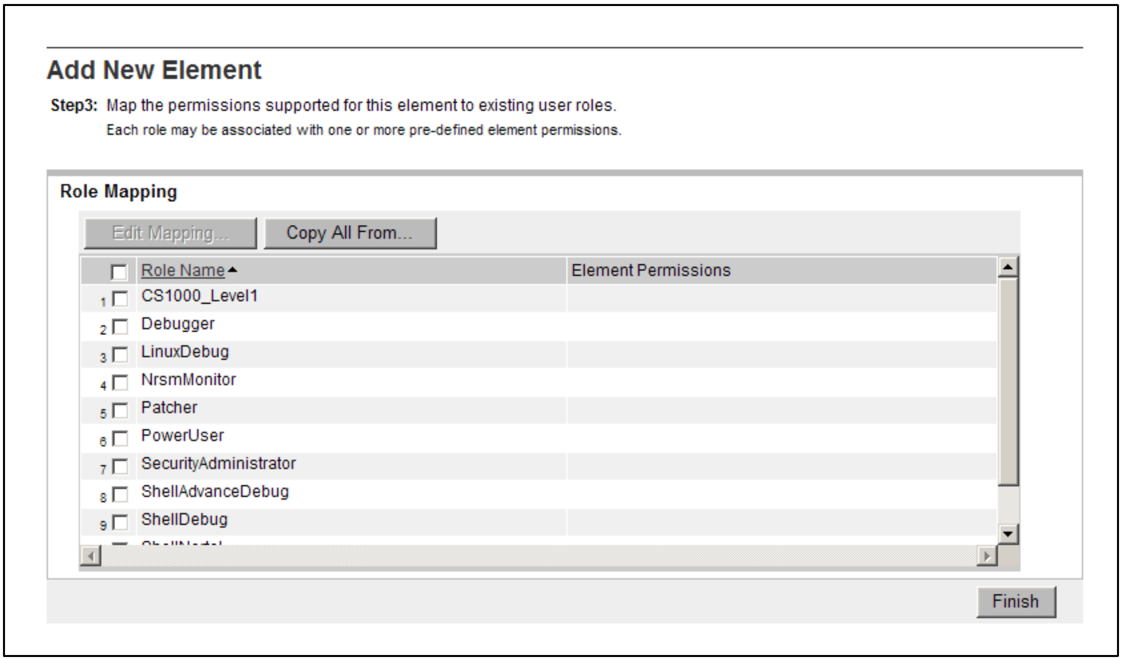
Step	Action

1 Add the new element in ECM as follows:

- To add a CS 1000 Release 5 element in ECM, follow the steps in Procedure 12 "Adding a CS 1000 Release 5 element" (page 55).
- To add a Network Routing Service element in ECM, follow the steps in Procedure 13 "Adding a Network Routing Service element" (page 60).
- To add a SIP Gateway element in ECM, follow the steps in Procedure 14 "Adding a SIP Gateway element" (page 63).

The **Add New Element Step 3** Web page appears, as shown in Figure 22 "Add New Element Step 3 Web page" (page 71).

Figure 22
Add New Element Step 3 Web page



Add New Element

Step3: Map the permissions supported for this element to existing user roles.
Each role may be associated with one or more pre-defined element permissions.

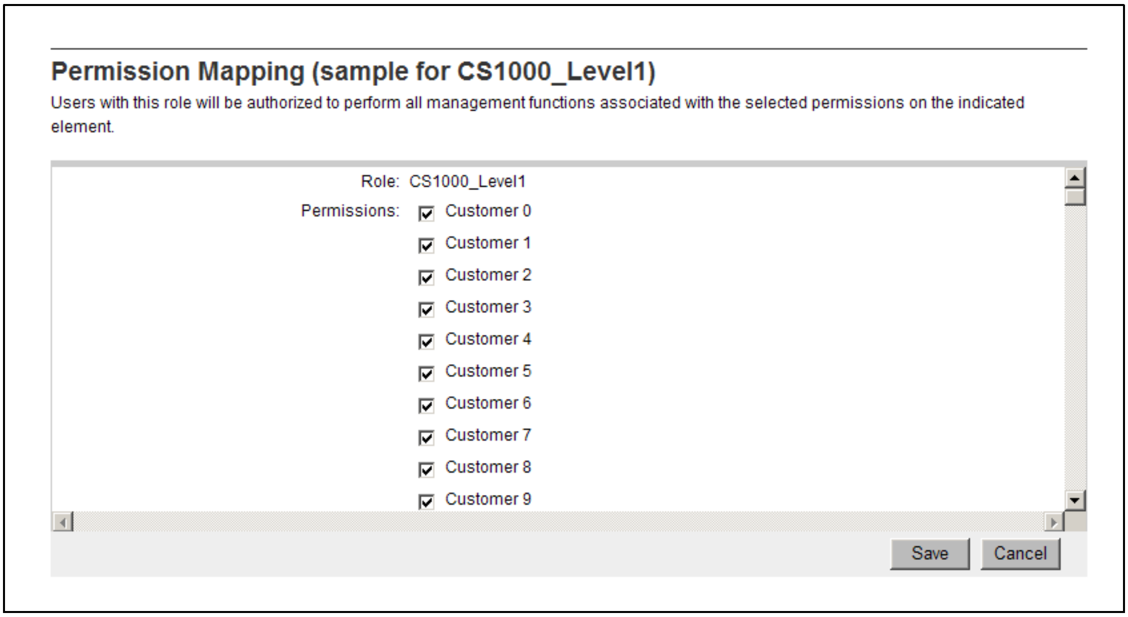
Role Mapping

	□	Role Name ▲	Element Permissions
1	□	CS1000_Level1	
2	□	Debugger	
3	□	LinuxDebug	
4	□	NrsmMonitor	
5	□	Patcher	
6	□	PowerUser	
7	□	SecurityAdministrator	
8	□	ShellAdvanceDebug	
9	□	ShellDebug	

2 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role, and click **Edit Mapping**.

The **Permission Mapping** Web page appears for the selected role, as shown in Figure 23 "Permission Mapping Web page" (page 72)

Figure 23
Permission Mapping Web page



Permission Mapping (sample for CS1000_Level1)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Role: CS1000_Level1

Permissions:
☑ Customer 0
☑ Customer 1
☑ Customer 2
☑ Customer 3
☑ Customer 4
☑ Customer 5
☑ Customer 6
☑ Customer 7
☑ Customer 8
☑ Customer 9

Select or clear the permissions for the element.

3 Click **Save**.

The **Add New Element Step 3** Web page appears. Users can select a different role to map permissions to the element.

4 Click **Finish**.

—End—

Edit element role mapping with Copy All From

Use the steps in Procedure 21 "Editing element role mapping with Copy All From for a new element" (page 72) to edit a CS 1000 Release 5, Network Routing Service, or SIP Gateway element role mapping with Copy All From.

Procedure 21
Editing element role mapping with Copy All From for a new element

Step Action

1 Add the new element in ECM as follows:

- To add a CS 1000 Release 5 element in ECM, follow the steps in Procedure 12 "Adding a CS 1000 Release 5 element" (page 55).

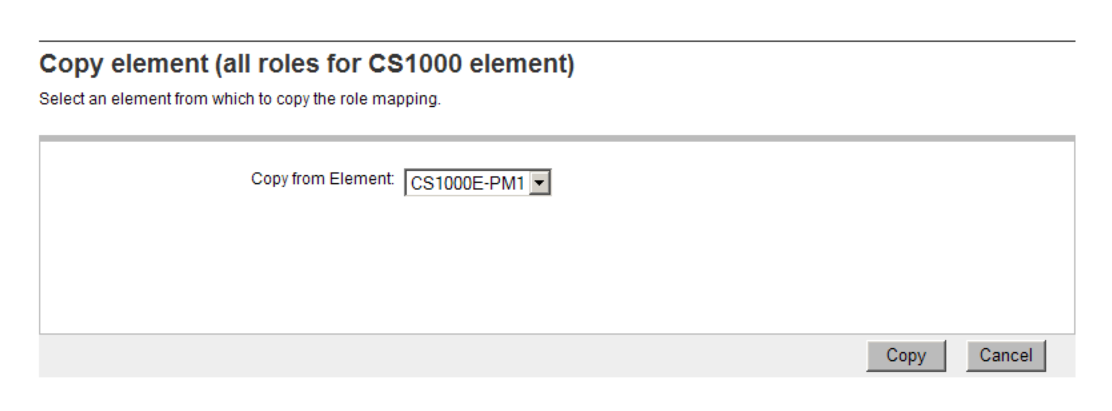
- To add a Network Routing Service element in ECM, follow the steps in Procedure 13 "Adding a Network Routing Service element" (page 60).
- To add a SIP Gateway element in ECM, follow the steps in Procedure 14 "Adding a SIP Gateway element" (page 63).

The **Add New Element Step 3** Web page appears, as shown in Figure 22 "Add New Element Step 3 Web page" (page 71).

2 From the **Add New Element Step 3** Web page, in the **Role Mapping** section, select a role, and click **Copy All From**.

The **Copy element** Web page appears, as shown in Figure 24 "Copy element Web page" (page 73).

Figure 24
Copy element Web page



Copy element (all roles for CS1000 element)

Select an element from which to copy the role mapping.

Copy from Element: CS1000E-PM1

3 From the **Copy element** Web page, from the **Copy from Element** list, select a role to copy for the element.

4 Click **Copy**.

5 Click **Finish**.

—End—

Edit element permission role assignments when editing a new element

Use these procedures to select or clear the permissions for an element role using Edit Mapping or Copy All From.

Assign permissions to roles to authorize users to perform management functions associated with the selected permissions when they access an element.

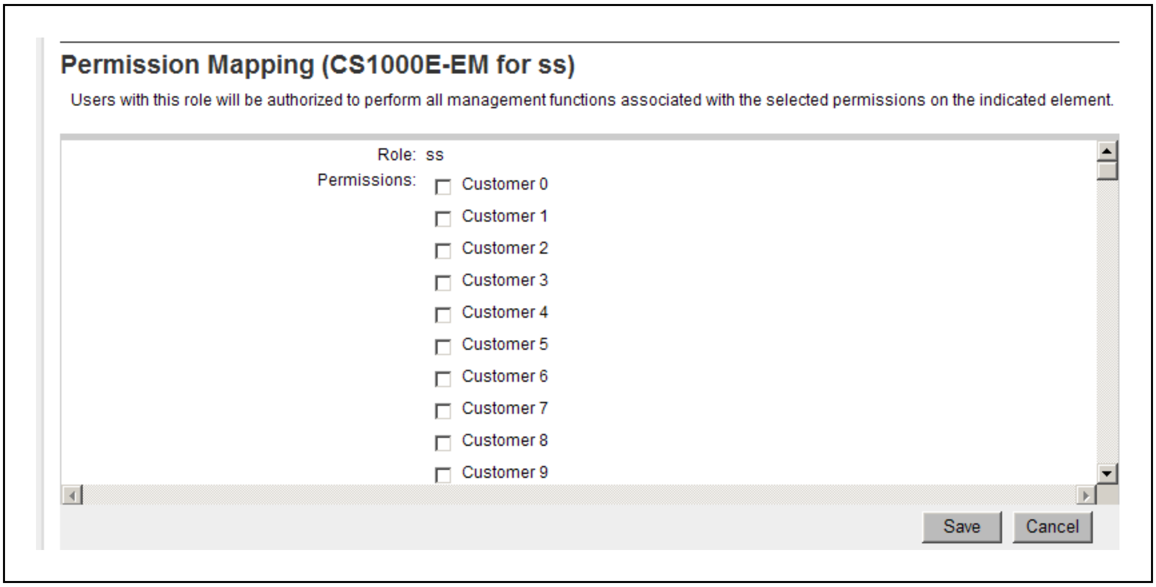
Edit element role permission mapping with Edit Mapping when editing a new element

Use the steps in Procedure 22 "Editing element permissions with Edit Mapping for a new element" (page 74) to edit element role mapping using Edit Mapping for a new element in ECM.

Procedure 22
Editing element permissions with Edit Mapping for a new element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	Select the check box beside an element to edit, and click **Edit**. The **Element Details** Web page appears.
4	From the **Element Details** Web page, in the **Role Mapping** section, select the check box beside a role, and click **Edit Mapping**, as shown in Figure 17 "Element Details Web page" (page 65). The **Permission Mapping** Web page appears, as shown in Figure 25 "Permission Mapping Web page" (page 74)

Figure 25
Permission Mapping Web page



Permission Mapping (CS1000E-EM for ss)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Role: ss

Permissions:
- □ Customer 0
- □ Customer 1
- □ Customer 2
- □ Customer 3
- □ Customer 4
- □ Customer 5
- □ Customer 6
- □ Customer 7
- □ Customer 8
- □ Customer 9

Step	Action
5	Select or clear the permissions for the element.

6 Click **Save**.

—End—

Edit element role permission mapping with Copy All From when editing a new element

Use the steps in Procedure 23 "Editing element role mapping with Copy All From for a new element" (page 75) to edit element role permissions using Copy All From for a new element in ECM.

Procedure 23

Editing element role permission mapping with Copy All From for a new element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 8 "Elements Web page" (page 52).
3	Select the check box beside an element to edit, and click **Edit**. The **Element Details** Web page appears, as shown in Figure 17 "Element Details Web page" (page 65).
4	From the **Element Details** Web page, select a role, and click **Copy All From**.
5	Select an element to copy from.
6	Click **Save**.

—End—

Assign default permissions to built-in roles when a new element is added

Use the steps in Procedure 24 "Assigning default permissions to built-in roles for a new element" (page 76) to assign default permissions to built-in roles when adding a new element in ECM.

Procedure 24
Assigning default permissions to built-in roles for a new element

Step Action

1 Add the new element in ECM as follows:

- To add a CS 1000 Release 5 element in ECM, follow the steps in Procedure 12 "Adding a CS 1000 Release 5 element" (page 55).
- To add a Network Routing Service element in ECM, follow the steps in Procedure 13 "Adding a Network Routing Service element" (page 60).
- To add a SIP Gateway element in ECM, follow the steps in Procedure 14 "Adding a SIP Gateway element" (page 63).

The **Add New Element Step 3** Web page appears, as shown in Figure 22 "Add New Element Step 3 Web page" (page 71).

2 From the **Add New Element Step 3** Web page, in the **Role Mapping** section, select the roles to assign the permissions supported for the element to the existing user roles.

3 Click **Finish**.

—End—

Security

Contents

This chapter contains the following topics:

This chapter discusses the following security features from the Security branch in the Enterprise Common Manager (ECM) navigation pane.

- Password
- Users
- Roles
- Sessions
- Policies
- Certificates

ECM provides the tools security administrators need to manage and maintain security within their ECM infrastructure. From the security section, a security administrator can perform the following tasks:

- view and change a local account password
- manage users and roles
- view and terminate active sessions
- configure the authentication scheme, authentication servers, passwords, and login warning banner policies
- manage certificates

  For information about how to manage certificates in ECM, see *Security Management Fundamentals (NN43001-604)*.

Use the procedures in this chapter to manage security in ECM.

Password

When the user clicks the Password link in the Security branch of the ECM navigator, the Password Web page appears. From the Password Web page, users can view the status for a local account password and change a local account password.

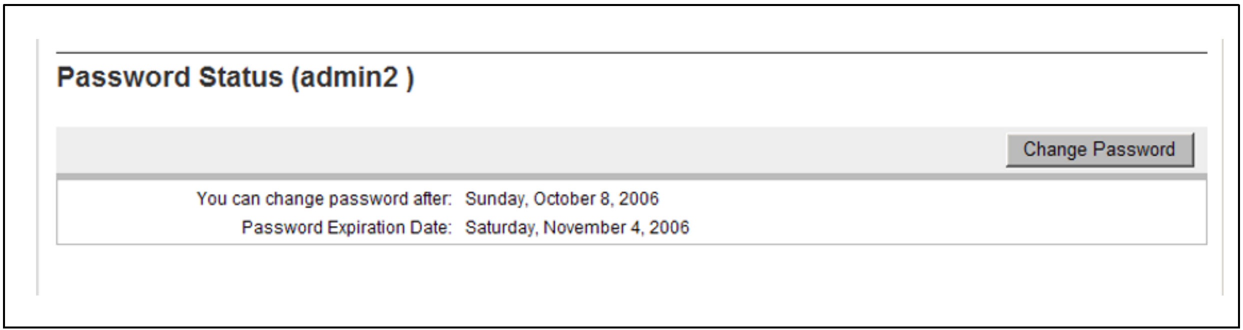
Review the status of a local account password

Use the steps in Procedure 25 "Reviewing the status of a local account password" (page 79) to determine when a local password can change and when the password expires.

Procedure 25
Reviewing the status of a local account password

Step	Action
1	Log on to the ECM framework.
2	From the navigation pane, click **Security** > **Password**. The **Password Status** Web page appears, as shown in Figure 26 "Password Status Web page" (page 79).

Figure 26
Password Status Web page



Password Status (admin2)

You can change password after: Sunday, October 8, 2006
Password Expiration Date: Saturday, November 4, 2006

ATTENTION
An external user cannot review or change the password.

—End—

Change a local account password

Use the steps in Procedure 26 "Changing a local account password" (page 79) to change the current password.

Procedure 26
Changing a local account password

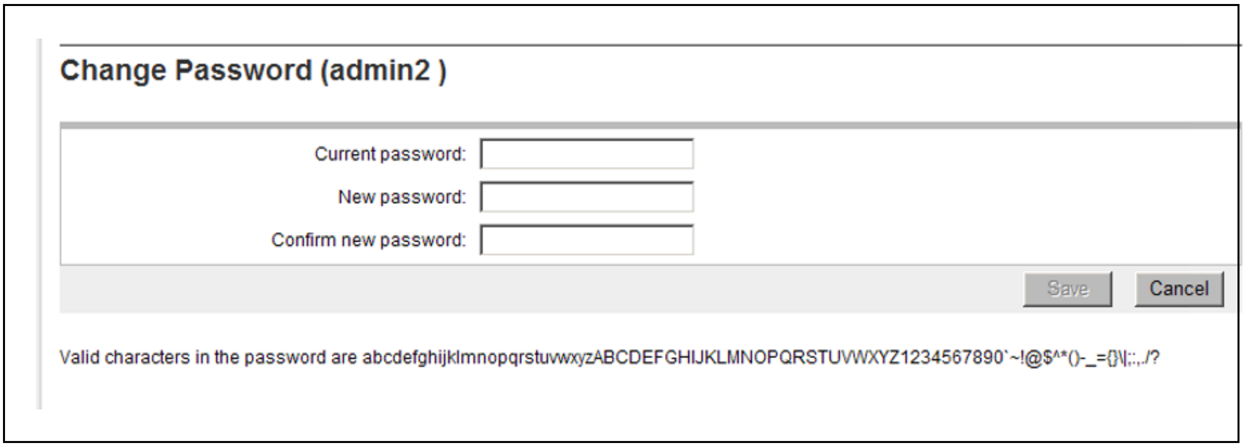
Step	Action
1	Log on to the ECM framework.
2	From the navigation pane, click **Security** > **Password**.

The **Password Status** Web page appears, as shown in Figure 26 "Password Status Web page" (page 79).

3 Click **Change Password**.

The **Change Password** Web page appears, as shown in Figure 27 "Change Password Web page" (page 80)

Figure 27
Change Password Web page



Change Password (admin2)

Current password:
New password:
Confirm new password:

Valid characters in the password are abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890`~!@$^*()-_={}\|;:,./?

4 In the **Current password** field, type the current password.

5 In the **New password** field, type the new password.

6 In the **Confirm new password** field, type the new password.

7 Click **Save**.

—End—

Users

When the user clicks the Users link in the Security branch of the ECM navigator, the Administrative Users Web page appears. From the Administrative Users Web page, security administrators can perform the various user management tasks required to manage users within ECM.

Review existing users

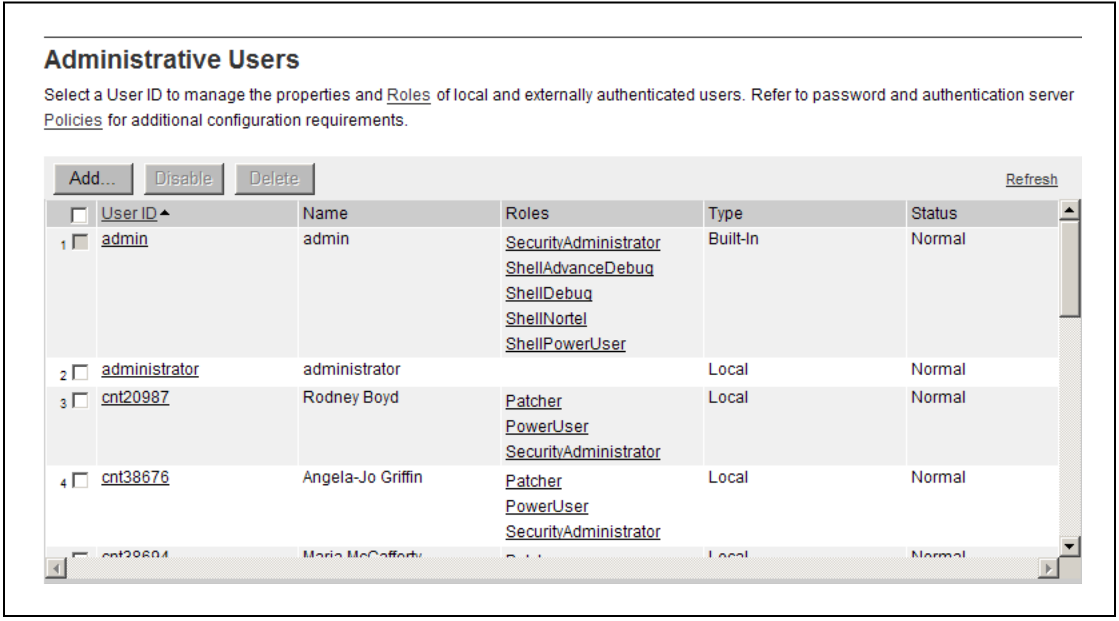
Use the steps in Procedure 27 "Reviewing existing users" (page 81) to view the users that are currently in ECM.

Procedure 27
Reviewing existing users

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**.

The **Administrative Users** Web page lists users within ECM. The User ID, name, roles, type, and status are displayed, as shown in Figure 28 "Administrative Users Web page" (page 81).

Figure 28
Administrative Users Web page



Administrative Users

Select a User ID to manage the properties and Roles of local and externally authenticated users. Refer to password and authentication server Policies for additional configuration requirements.

	□ User ID ▲	Name	Roles	Type	Status
1	□ admin	admin	SecurityAdministrator ShellAdvanceDebug ShellDebug ShellNortel ShellPowerUser	Built-In	Normal
2	□ administrator	administrator		Local	Normal
3	□ cnt20987	Rodney Boyd	Patcher PowerUser SecurityAdministrator	Local	Normal
4	□ cnt38676	Angela-Jo Griffin	Patcher PowerUser SecurityAdministrator	Local	Normal
	□ cnt38694	Maria McCafferty		Local	Normal

Step	Action
3	Review the information for existing users.

—End—

Add a new local user

Use the steps in Procedure 28 "Adding a new local user" (page 81) to add a new local user to ECM.

Procedure 28
Adding a new local user

Step	Action
1	Log on to ECM as a security administrator.

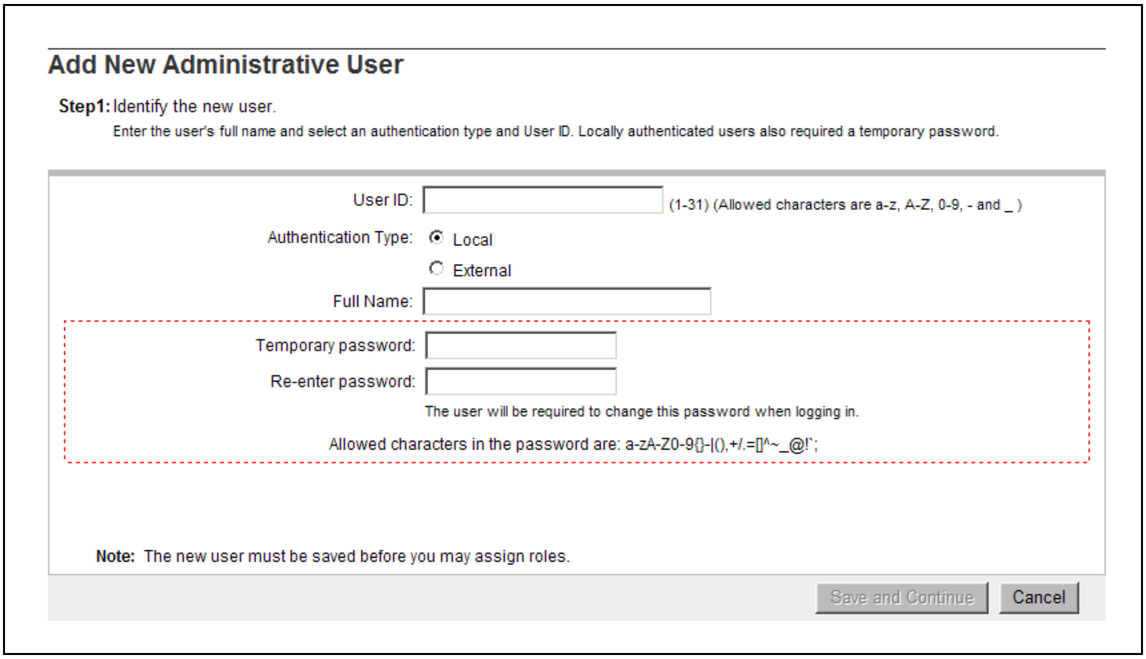
2 From the navigation pane, click **Security** > **Users**.

The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).

3 Click **Add**.

The **Add New Administrative User Step 1** Web page appears, as shown in Figure 29 "Add New Administrative User Step 1 Web page" (page 82).

Figure 29
Add New Administrative User Step 1 Web page



Add New Administrative User

Step1: Identify the new user.

Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

User ID: (1-31) (Allowed characters are a-z, A-Z, 0-9, - and _)

Authentication Type: ● Local ○ External

Full Name:

Temporary password:

Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9{}-|(),+/.=[]^~_@!`;

Note: The new user must be saved before you may assign roles.

4 From the **Authentication Type**, select **Local**.

5 In the **Full Name** field, type the name of the user.

6 In the **Temporary password** field, type the new password.

7 In the **Re-enter password** field, type the new password.

8 Click **Save and Continue**.

ATTENTION

The password that is entered for the new local user is temporary. When the new user logs on to ECM for the first time, they are required to change the password. Therefore, Nortel recommends that users record the new password in a secure place.

—End—

Add a new external user

Use the steps in Procedure 29 "Adding a new external user" (page 83) to add a new external user in ECM.

Procedure 29

Adding a new external user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click **Add**. The **Add New Administrative User** Web page appears, as shown in Figure 29 "Add New Administrative User Step 1 Web page" (page 82).
4	From the **Authentication Type**, select **External**.
5	In the **User ID** field, type the user ID.
6	Click **Save and Continue**.

—End—

ATTENTION

To prevent an external RADIUS or LDAP account from being locked, make sure that local accounts in ECM do not have the same login name in the external RADIUS and LDAP servers. Also, when the external RADIUS and LDAP external servers are both enabled, make sure there are no common login names in these servers.

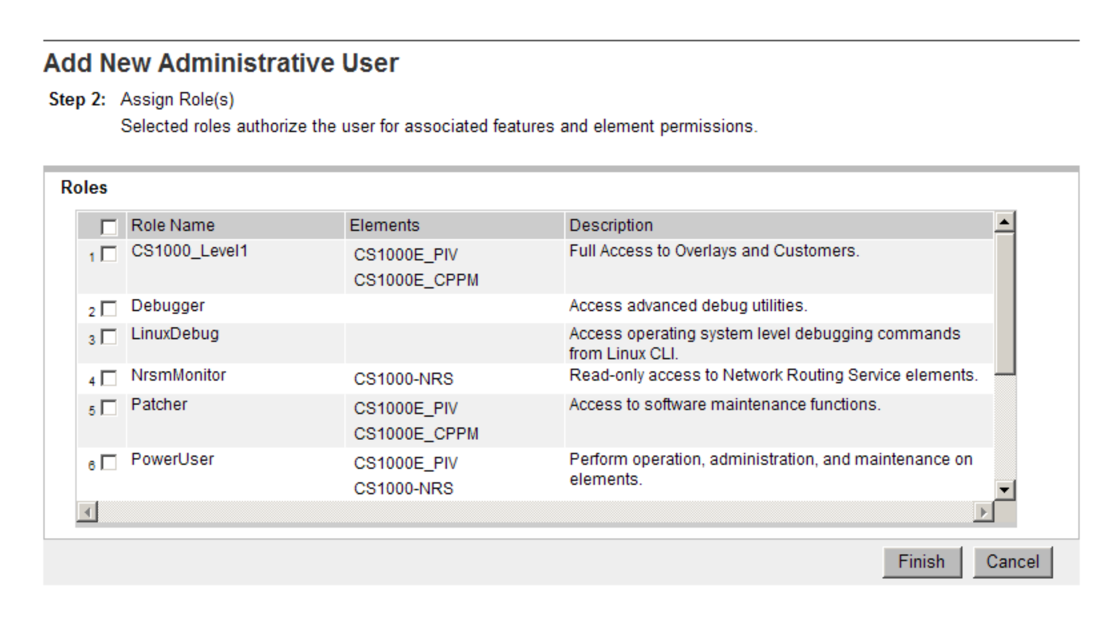
Add user role assignments for a local user when a new user is added

Use the steps in Procedure 30 "Assigning a user role to a new local user" (page 84) to assign a user role when you add a new local user.

Procedure 30
Assigning a user role to a new local user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click **Add**. The **Add New Administrative User** Web page appears, as shown in Figure 29 "Add New Administrative User Step 1 Web page" (page 82).
4	From the **Authentication Type**, select **Local**.
5	In the **Full Name** field, type the name of the user.
6	In the **Temporary password** field, type the new password.
7	In the **Re-enter password** field, type the new password.
8	Click **Save and Continue**. The **Add New Administrative User Step 2** Web page appears, as shown in Figure 30 "Add New Administrative User Step 2 Web page" (page 84).

Figure 30
Add New Administrative User Step 2 Web page



Add New Administrative User

Step 2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.

Roles

	□	Role Name	Elements	Description
1	□	CS1000_Level1	CS1000E_PIV CS1000E_CPPM	Full Access to Overlays and Customers.
2	□	Debugger		Access advanced debug utilities.
3	□	LinuxDebug		Access operating system level debugging commands from Linux CLI.
4	□	NrsmMonitor	CS1000-NRS	Read-only access to Network Routing Service elements.
5	□	Patcher	CS1000E_PIV CS1000E_CPPM	Access to software maintenance functions.
6	□	PowerUser	CS1000E_PIV CS1000-NRS	Perform operation, administration, and maintenance on elements.

9 From the **Role Name** column, select the check box beside the role or roles to assign to the new local user.

10 Click **Finish**.

—End—

Add user role assignments for an external user when a new user is added

Use the steps in Procedure 31 "Assigning a user role to a new external user" (page 85) to assign a user role when you add a new external user.

Procedure 31
Assigning a user role to a new external user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click **Add**. The **Add New Administrative User** Web page appears as shown in Figure 29 "Add New Administrative User Step 1 Web page" (page 82).
4	From the **Authentication Type**, select **External**.
5	In the **User ID** field, type the user ID.
6	Click **Save and Continue**. The **Add New Administrative User Step 2** Web page appears, as shown in Figure 30 "Add New Administrative User Step 2 Web page" (page 84).
7	From the **Role Name** column, select the role or roles to assign to the new external user.
8	Click **Finish**.

—End—

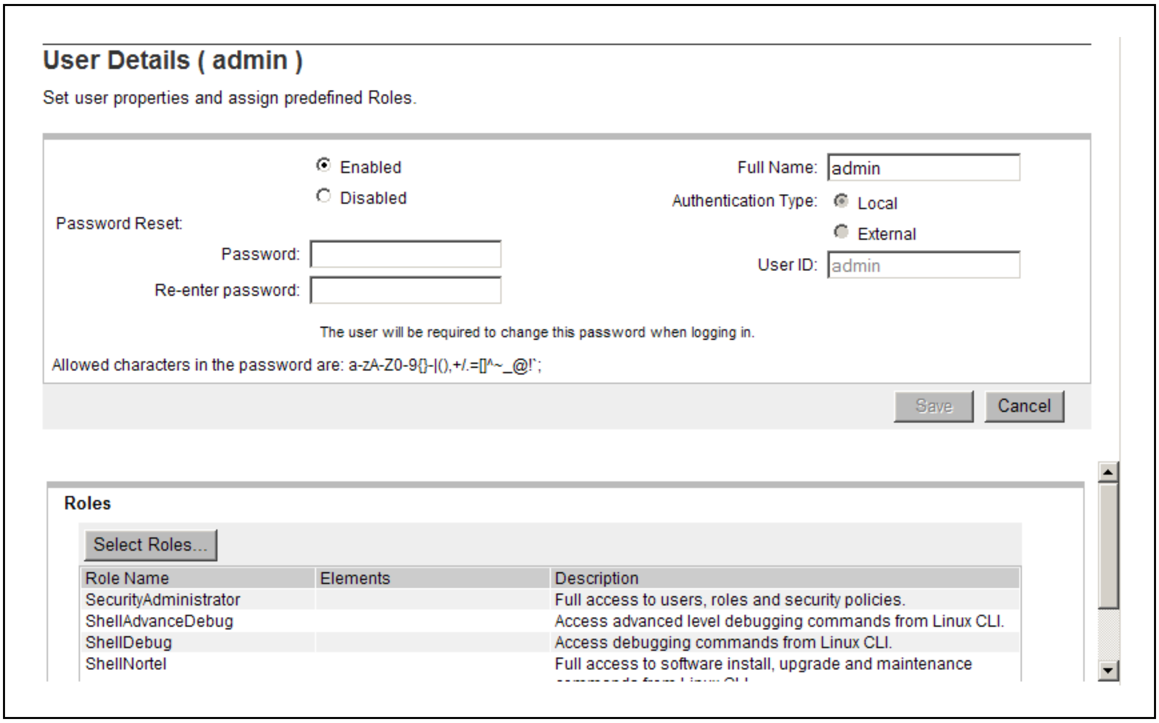
Edit user role mapping

Use the steps in Procedure 32 "Editing user role mapping" (page 86) to select roles to authorize a user for associated features and element permissions.

Procedure 32
Editing user role mapping

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click the name of a user to edit the user role mapping. The **User Details** Web page appears, as shown in Figure 31 "User Details Web page" (page 86)

Figure 31
User Details Web page



User Details (admin)

Set user properties and assign predefined Roles.

● Enabled
○ Disabled

Full Name: admin

Authentication Type: ● Local ○ External

User ID: admin

Password Reset:

Password:

Re-enter password:

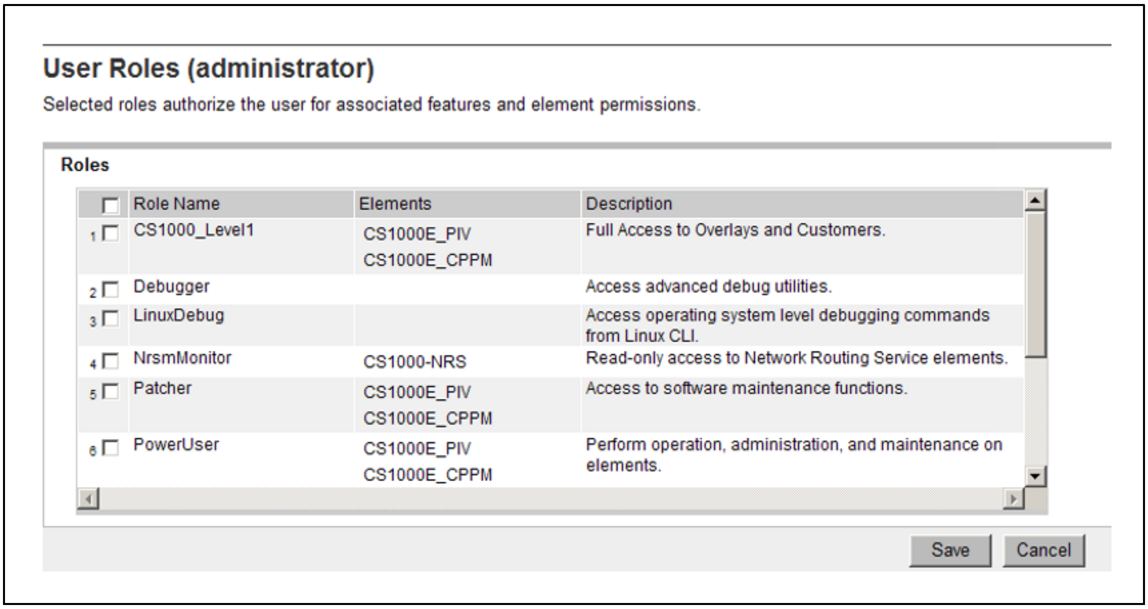
The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9{}-|(),+/.=[]^~_@!`;

Role Name	Elements	Description
SecurityAdministrator		Full access to users, roles and security policies.
ShellAdvanceDebug		Access advanced level debugging commands from Linux CLI.
ShellDebug		Access debugging commands from Linux CLI.
ShellNortel		Full access to software install, upgrade and maintenance

Step	Action
4	Click **Select Roles**. The **User Roles** Web page appears for the selected user, as shown in Figure 32 "User Roles Web page" (page 87).

Figure 32
User Roles Web page



User Roles (administrator)

Selected roles authorize the user for associated features and element permissions.

Roles

☐	Role Name	Elements	Description
1 ☐	CS1000_Level1	CS1000E_PIV CS1000E_CPPM	Full Access to Overlays and Customers.
2 ☐	Debugger		Access advanced debug utilities.
3 ☐	LinuxDebug		Access operating system level debugging commands from Linux CLI.
4 ☐	NrsmMonitor	CS1000-NRS	Read-only access to Network Routing Service elements.
5 ☐	Patcher	CS1000E_PIV CS1000E_CPPM	Access to software maintenance functions.
6 ☐	PowerUser	CS1000E_PIV CS1000E_CPPM	Perform operation, administration, and maintenance on elements.

5 Select the roles for the selected user.

6 Click **Save**.

—End—

Configure the properties of a local user

A security administrator can edit the full name and reset the password for local and built-in administrators. A security administrator can also, enable or disable accounts and edit the selected administrator’s role assignment.

Use the following procedures to change the full name and password for a local user, to disable and enable a local user account, and to delete a user.

Edit the full name for a local user account

Use the steps in Procedure 33 "Editing the full name of a local user account" (page 87) to change the full name for a local user account.

Procedure 33
Editing the full name of a local user account

Step Action

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Users**.

The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).

3 Click the name of the user.

The **User Details** Web page appears, as shown in Figure 31 "User Details Web page" (page 86).

4 In the **Full Name** field, type the name.

5 Click **Save**.

—End—

Reset the password for a local user account

Use the steps in Procedure 34 "Resetting the password for a local user account" (page 88) to reset the password for a local user account.

Procedure 34
Resetting the password for a local user account

Step	Action

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Users**.

The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).

3 Click the name of the user.

The **User Details** Web page appears, as shown in Figure 31 "User Details Web page" (page 86).

4 In the **Password Reset** section, in the **Password** field, enter the new password.

5 In the **Re-enter password** field, type the new password.

6 Click **Save**.

7 Log on as the selected user.

—End—

Disable a user account

Use the steps in Procedure 35 "Disabling a user account" (page 89) to disable a user account within ECM.

Procedure 35
Disabling a user account

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Select the check box beside a user name, and click **Disable**. Log on as the selected user to verify the change. A user can disable built-in accounts; however, the ECM security framework does not notify the Linux servers when this occurs. The built-in accounts are still valid in the Linux host account database.

—End—

Enable a user account

Use the steps in Procedure 36 "Enabling a user account" (page 89) to enable a user account within ECM.

Procedure 36
Enabling a user account

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click the user ID for the disabled user account. The **User Details** Web page appears, as shown in Figure 31 "User Details Web page" (page 86).
4	From the **User Details** Web page, select **Enabled**.

—End—

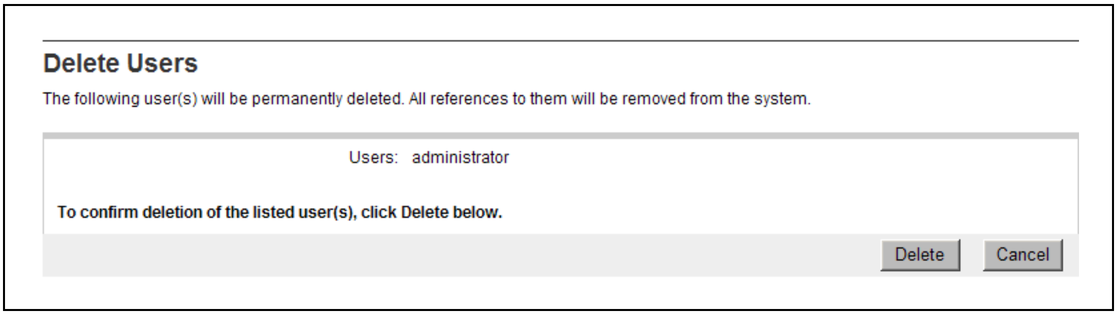
Delete a user

Use the steps in Procedure 37 "Deleting a user" (page 90) to delete a user in ECM.

Procedure 37
Deleting a user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Users**. The **Administrative Users** Web page appears, as shown in Figure 28 "Administrative Users Web page" (page 81).
3	Click the check box beside the name of the user.
4	Click **Delete**. The **Delete Users** Web page appears, as shown in Figure 33 "Delete Users Web page" (page 90).

Figure 33
Delete Users Web page



Delete Users

The following user(s) will be permanently deleted. All references to them will be removed from the system.

Users: administrator

To confirm deletion of the listed user(s), click Delete below.

5 Click **Delete** to proceed with the deletion or **Cancel** to cancel the deletion.

> **ATTENTION**
> Users cannot delete their own account.

—End—

Roles

When the user clicks the Roles link in the Security branch of the ECM navigator, the Roles Web page appears. From the Roles Web page, security administrators can perform the various role management tasks required to manage roles within ECM.

The ECM security framework supports built-in and custom roles. The built-in roles provide default access control policies for assigned users. Users create custom roles to provide more options for access control to managed elements.

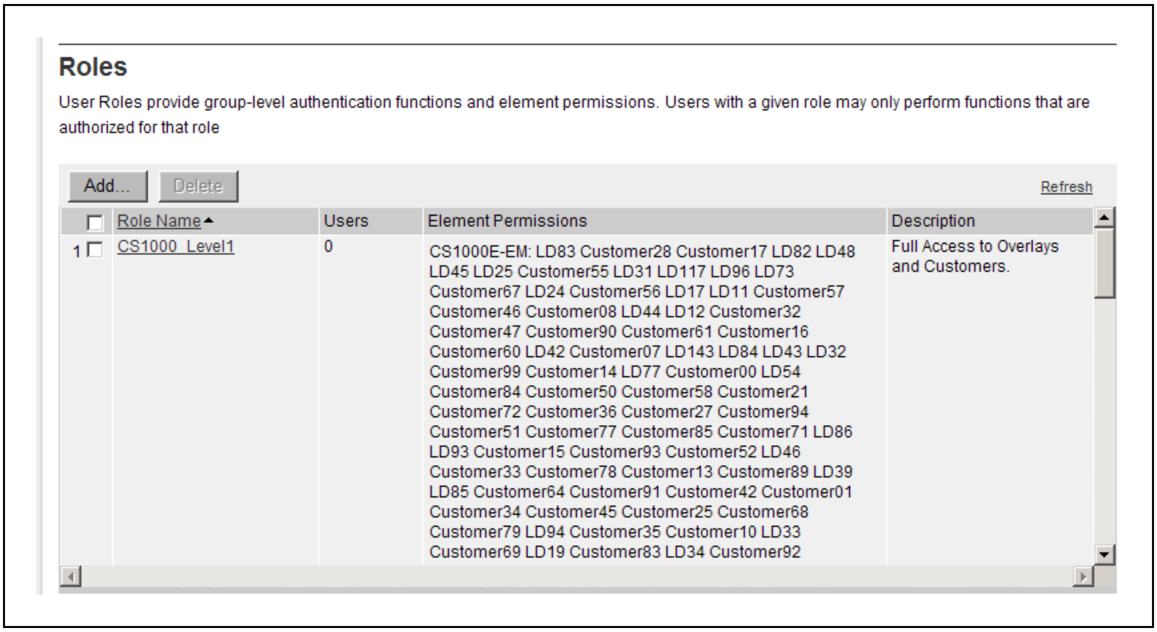
Review existing roles

Use the steps in Procedure 38 "Reviewing existing roles" (page 91) to view the current roles in ECM.

Procedure 38
Reviewing existing roles

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Roles**. The **Roles** Web page appears with a list of available roles, as shown in Figure 34 "Roles Web page" (page 91).

Figure 34
Roles Web page



Roles

User Roles provide group-level authentication functions and element permissions. Users with a given role may only perform functions that are authorized for that role

	□ Role Name	Users	Element Permissions	Description
1	□ CS1000_Level1	0	CS1000E-EM: LD83 Customer28 Customer17 LD82 LD48 LD45 LD25 Customer55 LD31 LD117 LD96 LD73 Customer67 LD24 Customer56 LD17 LD11 Customer57 Customer46 Customer08 LD44 LD12 Customer32 Customer47 Customer90 Customer61 Customer16 Customer60 LD42 Customer07 LD143 LD84 LD43 LD32 Customer99 Customer14 LD77 Customer00 LD54 Customer84 Customer50 Customer58 Customer21 Customer72 Customer36 Customer27 Customer94 Customer51 Customer77 Customer85 Customer71 LD86 LD93 Customer15 Customer93 Customer52 LD46 Customer33 Customer78 Customer13 Customer89 LD39 LD85 Customer64 Customer91 Customer42 Customer01 Customer34 Customer45 Customer25 Customer68 Customer79 LD94 Customer35 Customer10 LD33 Customer69 LD19 Customer83 LD34 Customer92	Full Access to Overlays and Customers.

3	Use the scroll bar to review the existing roles within ECM.

—End—

Add a new role

A security administrator can add new roles to the default list of roles currently in ECM to manage access control for users of their management system.

Use the steps in Procedure 39 "Adding a new role" (page 92) to add a new role for specific access control policies in ECM.

Procedure 39
Adding a new role

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Roles**. The **Roles** Web page appears with a list of available roles, as shown in Figure 34 "Roles Web page" (page 91).
3	Click **Add**.
4	In the **Role Name** field, type the unique role name.
5	In the **Role Description** field, type a description for the new role.
6	Click **Save and Continue**.

—End—

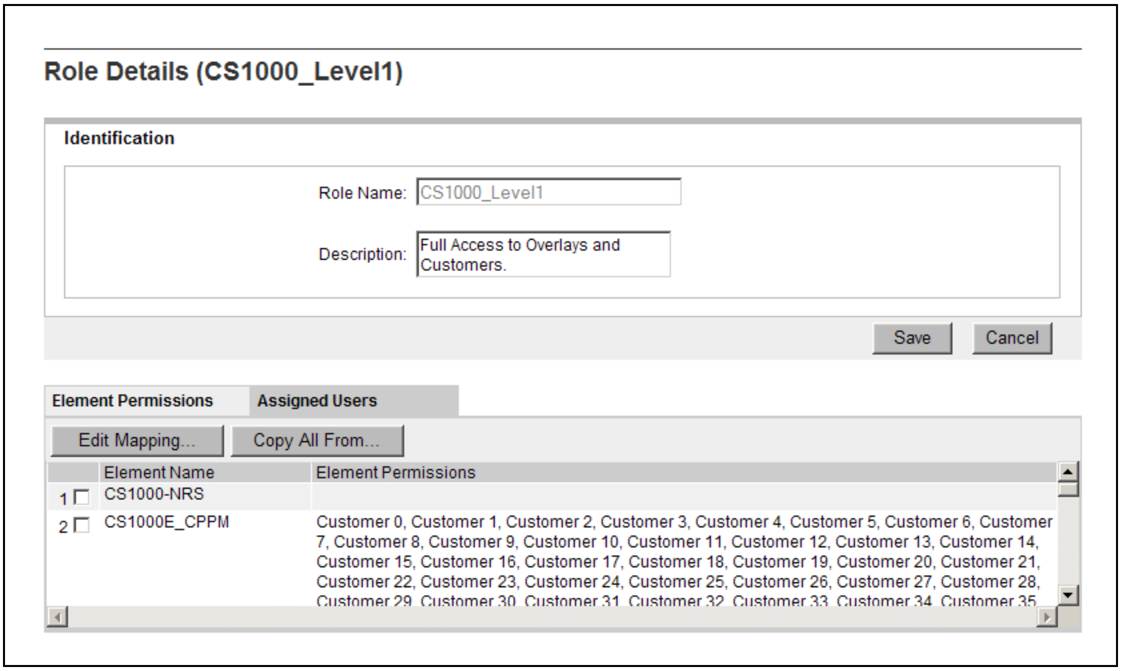
Edit a role description

Use the steps in Procedure 40 "Editing a role description" (page 92) to change the description for a role in ECM.

Procedure 40
Editing a role description

Step	Action
1	Log on to ECM.
2	From the navigation pane, click **Security** > **Roles**. The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91).
3	From the **Role Name** column, click a role to edit the description. The **Role Details** Web page appears. as shown in Figure 35 "Role Details Web page" (page 93).

Figure 35
Role Details Web page



Role Details (CS1000_Level1)

Identification

Role Name: CS1000_Level1

Description: Full Access to Overlays and Customers.

	Element Name	Element Permissions
1 □	CS1000-NRS	
2 □	CS1000E_CPPM	Customer 0, Customer 1, Customer 2, Customer 3, Customer 4, Customer 5, Customer 6, Customer 7, Customer 8, Customer 9, Customer 10, Customer 11, Customer 12, Customer 13, Customer 14, Customer 15, Customer 16, Customer 17, Customer 18, Customer 19, Customer 20, Customer 21, Customer 22, Customer 23, Customer 24, Customer 25, Customer 26, Customer 27, Customer 28, Customer 29 Customer 30 Customer 31 Customer 32 Customer 33 Customer 34 Customer 35

4 In the **Description** field, edit the information as required.

5 Click **Save**.

—End—

Edit role user mapping

Use the steps in Procedure 41 "Editing role user mapping" (page 93) to select users to grant the permissions associated with a selected role.

Procedure 41
Editing role user mapping

Step **Action**

1 Log on to ECM.

2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91).

3 From the **Role Name** column, click a role name.

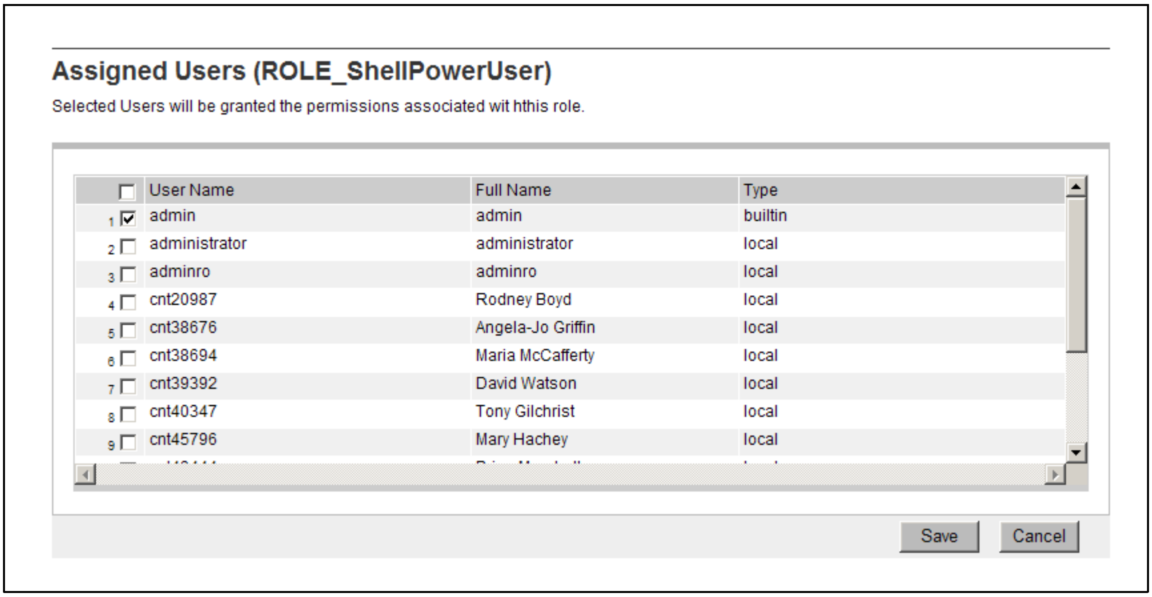
The **Role Details** Web page appears. as shown in Figure 35 "Role Details Web page" (page 93).

4 Click **Assigned Users**.

5 Click **Select Users**.

The **Assigned Users** Web page for the selected role appears, as shown in Figure 36 "Assigned Users Web page" (page 94)

Figure 36
Assigned Users Web page



Assigned Users (ROLE_ShellPowerUser)

Selected Users will be granted the permissions associated wit hthis role.

	□	User Name	Full Name	Type
1	☑	admin	admin	builtin
2	□	administrator	administrator	local
3	□	adminro	adminro	local
4	□	cnt20987	Rodney Boyd	local
5	□	cnt38676	Angela-Jo Griffin	local
6	□	cnt38694	Maria McCafferty	local
7	□	cnt39392	David Watson	local
8	□	cnt40347	Tony Gilchrist	local
9	□	cnt45796	Mary Hachey	local

6 Select the users to be granted the permissions associated with the selected role.

—End—

Copy all users from role

Use the steps in Procedure 42 "Copying all users from role" (page 94) to select a role to copy the list of assigned users.

Procedure 42
Copying all users from role

Step	Action
1	Log on to ECM.
2	From the navigation pane, click **Security** > **Roles**. The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91).
3	From the **Role Name** column, click a role name.

The **Role Details** Web page appears. as shown in Figure 35 "Role Details Web page" (page 93).

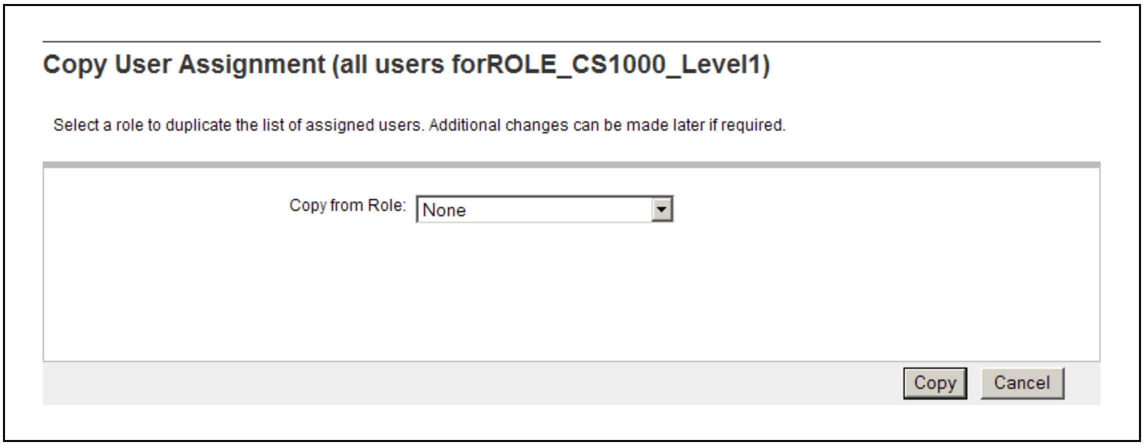
4 From the **Element Name** column, select the check box beside an element, and click **Assigned Users**.

5 Click **Select Users**.

6 Click **Copy All From**.

The **Copy User Assignment** Web page appears, as shown in Figure 37 "Copy User Assignment Web page" (page 95)

Figure 37
Copy User Assignment Web page



Copy User Assignment (all users forROLE_CS1000_Level1)

Select a role to duplicate the list of assigned users. Additional changes can be made later if required.

Copy from Role: None

7 Select a role from the **Copy from Role** list, and click **Copy**.

—End—

Edit role element permissions when adding a new role

Use these procedures to map element permissions for a new role with Edit Mapping and Copy All From. Users assigned to the new role are authorized to access functions according to the selected permissions for each element.

Edit role element permissions with Edit Mapping for a new role

Use the steps in Procedure 43 "Editing role element permissions with Edit Mapping " (page 95) to edit role element permissions with Edit Mapping for a new role in ECM.

Procedure 43
Editing role element permissions with Edit Mapping when adding a new role

Step **Action**

1 Log on to ECM as a security administrator.

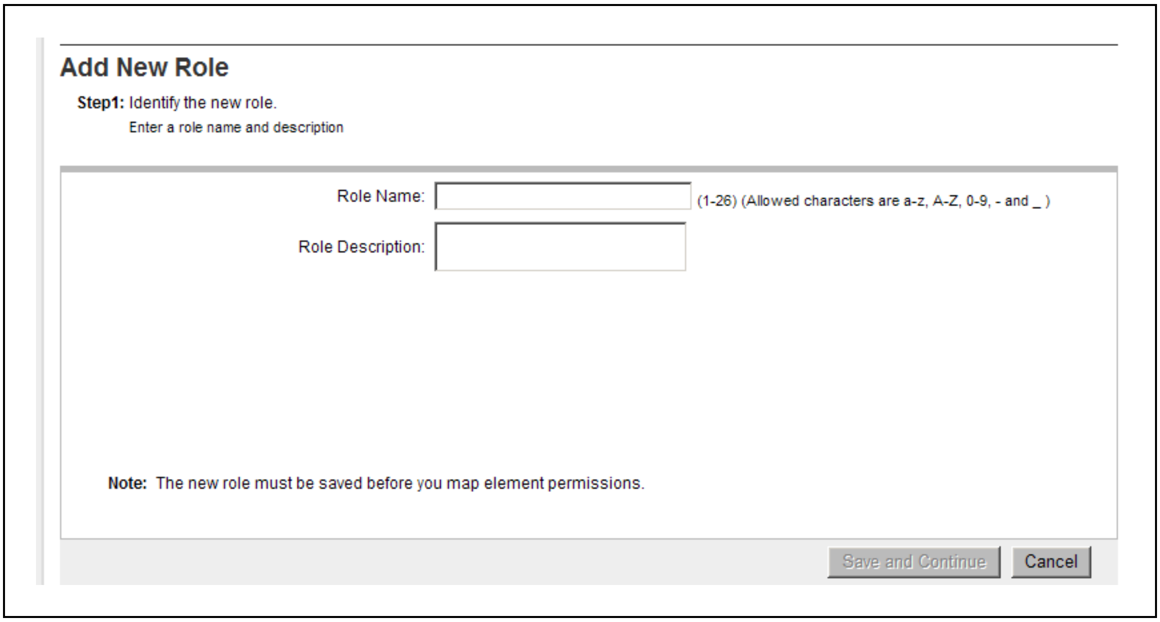
2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91).

3 Click **Add**.

The **Add New Role Step 1** Web page appears, as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).

Figure 38
Add New Role Step 1 Web page



Add New Role

Step1: Identify the new role.

Enter a role name and description

Role Name: (1-26) (Allowed characters are a-z, A-Z, 0-9, - and _)

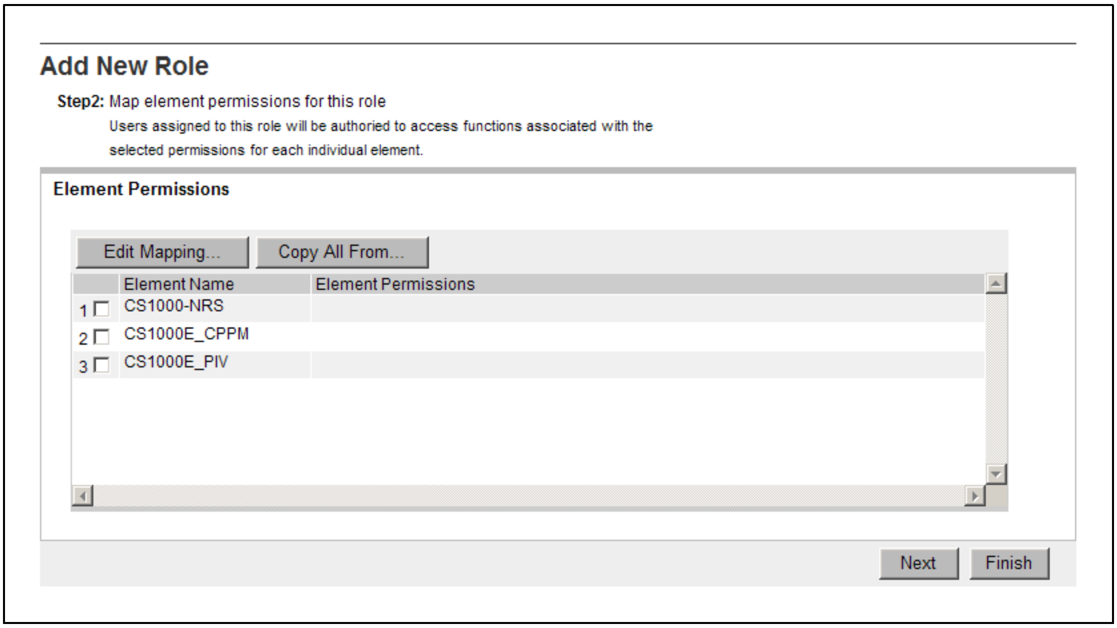
Role Description:

Note: The new role must be saved before you map element permissions.

4 Type the information for **Role Name** and **Role Description** as required, and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

Figure 39
Add New Role Step 2 Web page



Add New Role

Step2: Map element permissions for this role

Users assigned to this role will be authoried to access functions associated with the selected permissions for each individual element.

Element Permissions

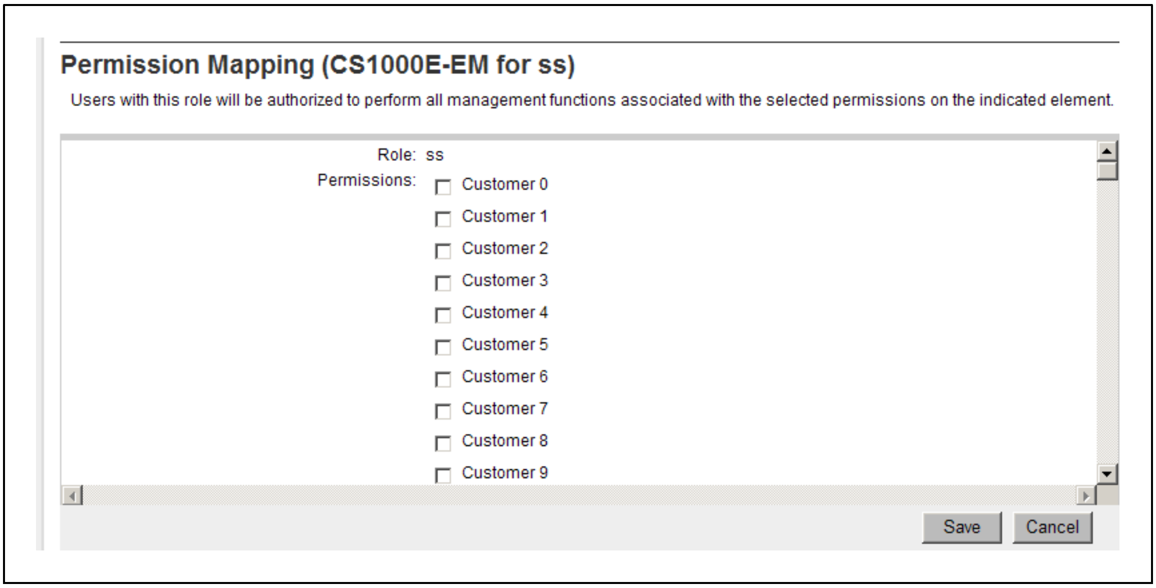
	Element Name	Element Permissions
1 □	CS1000-NRS	
2 □	CS1000E_CPPM	
3 □	CS1000E_PIV	

5 From the **Add New Role Step 2** Web page, in the **Elements Permission** section, select a check box beside an element name, and click **Edit Mapping**.

The **Permission Mapping** Web page appears for the selected element, as shown in Figure 40 "Permission Mapping Web page" (page 98).

Verify that the permissions for the element that are assigned to the new role are selected.

Figure 40
Permission Mapping Web page



Permission Mapping (CS1000E-EM for ss)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Role: ss

Permissions:

□ Customer 0
□ Customer 1
□ Customer 2
□ Customer 3
□ Customer 4
□ Customer 5
□ Customer 6
□ Customer 7
□ Customer 8
□ Customer 9

6 Click **Save**.

—End—

Edit role element permissions with Copy All From for a new role

Use the steps in Procedure 44 "Editing role element permissions with Copy All From" (page 98) to edit role element permissions with Copy All From for a new role in ECM.

Procedure 44
Editing role element permissions with Copy All From when adding a new role

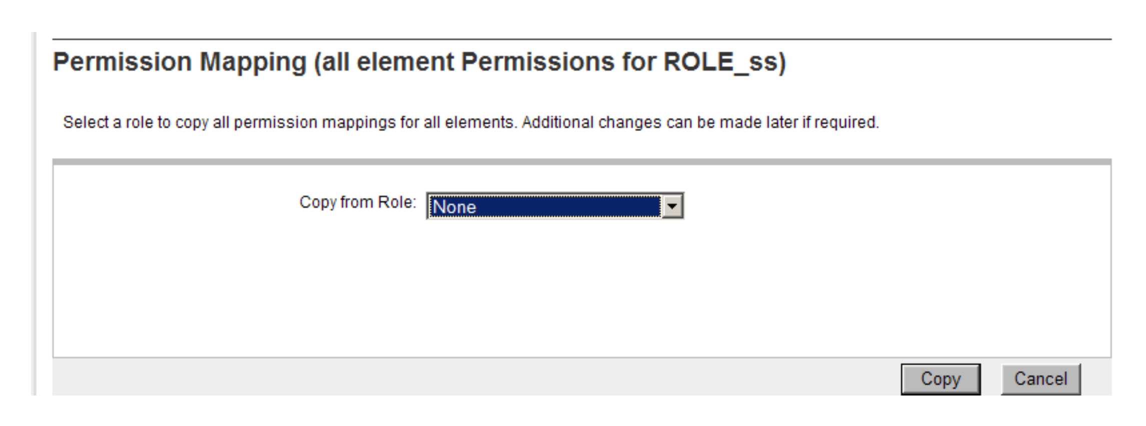
Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Roles**. The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91)
3	Click **Add**. The **Add New Role Step 1** Web page appears as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).
4	Enter the information for **Role Name** and **Role Description** as required and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

5 From the **Add New Role Step 2** Web page, in the **Elements Permission** section, click **Copy All From**, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

The **Permission Mapping** Web page appears, as shown in Figure 41 "Permission Mapping, Copy from Role Web page" (page 99).

Figure 41
Permission Mapping, Copy from Role Web page



Permission Mapping (all element Permissions for ROLE_ss)

Select a role to copy all permission mappings for all elements. Additional changes can be made later if required.

Copy from Role: None

6 From the **Copy from Role** list, select an element to copy from.

7 Click **Copy**.

—End—

Edit a role element permission for an existing role

Use these procedures to edit role element permissions for an existing role with Edit Mapping and Copy All From.

Edit a role element permission for an existing role with Edit Mapping

Use the steps in Procedure 45 "Editing a role element permission for an existing role with Edit Mapping" (page 99) to edit a role element permission using Edit Mapping.

Procedure 45
Editing a role element permission for an existing role with Edit Mapping

Step Action

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears as shown in Figure 34 "Roles Web page" (page 91).

3 Click **Add**.

The **Add New Role Step 1** Web page appears, as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).

4 Type the information for **Role Name** and **Role Description** as required, and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

5 From the **Add New Role Step 2** Web page, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97), click **Edit Mapping**.

6 Select or clear the permissions for the element.

7 Click **Save**.

—End—

Edit a role element permission for an existing role with Copy All From

Use the steps in Procedure 46 "Editing a role element permission for an existing role with Copy All From" (page 100) to edit a role element permission using Copy All From.

Procedure 46

Editing a role element permission for an existing role with Copy All From

Step Action

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91)

3 Click **Add**.

The **Add New Role Step 1** Web page appears, as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).

4 Type the information for **Role Name** and **Role Description** as required, and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

5 From the **Add New Role Step 2** Web page, in the **Element Permissions** section, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97), click **Copy All From**, .

6 Select or clear the permissions for the element.

7 Click **Copy**.

Verify the changes in the **Elements Permissions**.

—End—

Edit a role user assignment when adding a new role

Use these procedures to assign users to a new role. The assigned users are authorized to access functions associated with the selected permissions for each element.

Edit a role user assignment when adding a new role with Select Users

Use the steps in Procedure 47 "Editing a role user assignment with Select Users" (page 101) to edit a role user assignment using select users.

Procedure 47
Editing a role user assignment with Select Users

Step **Action**

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91).

3 Click **Add**.

The **Add New Role Step 1** Web page appears, as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).

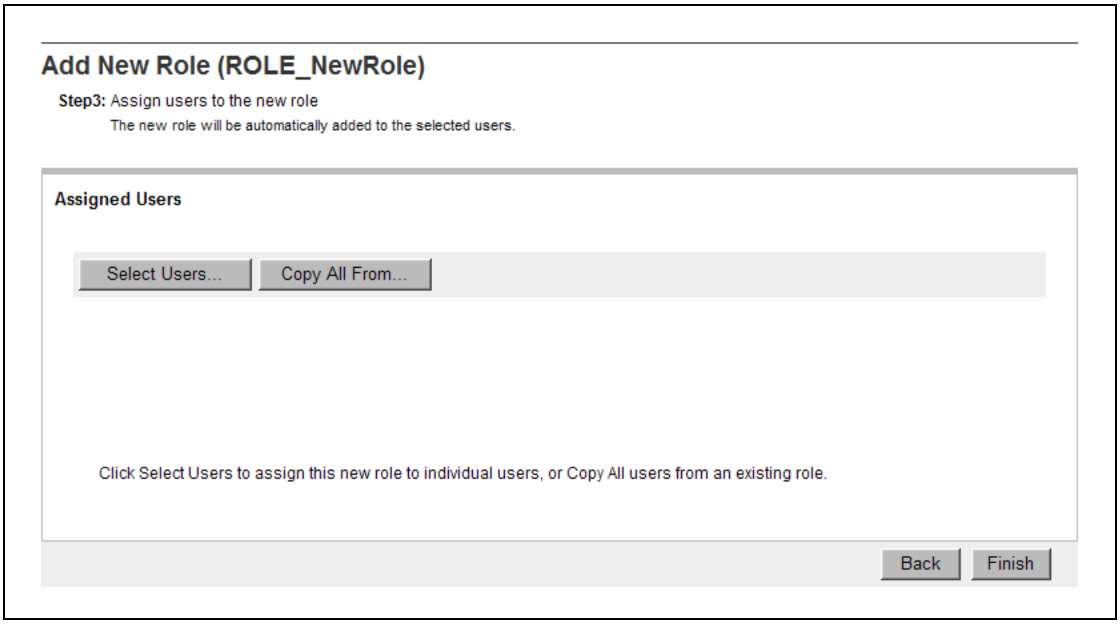
4 Type the information for **Role Name** and **Role Description** as required, and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

5 From the **Add New Role Step 2** Web page, in the **Elements Permission** section, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97), select an element name, and click **Next**,

6 From the **Add New Role Step 3**, as shown in Figure 42 "Add New Role Step 3" (page 102) Web page, click **Select Users**.

Figure 42
Add New Role Step 3



Add New Role (ROLE_NewRole)

Step3: Assign users to the new role

The new role will be automatically added to the selected users.

Assigned Users

Click Select Users to assign this new role to individual users, or Copy All users from an existing role.

Verify the users assigned to the new role are selected and edit as required.

7 Click **Save**.

—End—

Edit a role user assignment when adding a new role with Copy All From

Use the steps in Procedure 48 "Editing a role user assignment with Copy All From" (page 102) to edit a role user assignment using Copy All From.

Procedure 48
Editing a role user assignment with Copy All From

Step Action

1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Roles**.

The **Roles** Web page appears, as shown in Figure 34 "Roles Web page" (page 91)

3 Click **Add**.

The **Add New Role Step 1** Web page appears, as shown in Figure 38 "Add New Role Step 1 Web page" (page 96).

4 Enter the information for **Role Name** and **Role Description** as required, and click **Save and Continue**.

The **Add New Role Step 2** Web page appears, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97).

5 From the **Add New Role Step 2** Web page, in the **Elements Permission** section, as shown in Figure 39 "Add New Role Step 2 Web page" (page 97)select a check box beside an element name, and click **Next**.

6 From the **Add New Role Step 3** Web page, as shown in Figure 42 "Add New Role Step 3" (page 102), click **Copy All From**.

7 Select an element to copy from.

8 Click **Copy**.

—End—

Delete custom roles

Use the steps in Procedure 49 "Deleting custom roles" (page 103) to delete custom roles.

A user cannot delete built-in roles. A user who is logged on as security administrator can delete custom roles. User role assignments for administrators assigned to the deleted roles are also deleted.

Procedure 49
Deleting custom roles

Step Action

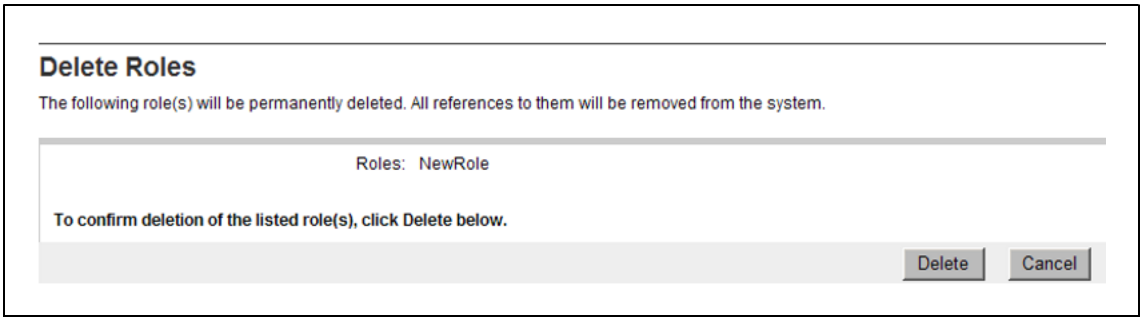
1 Log on to ECM as a security administrator.

2 From the navigation pane, click **Security** > **Roles**.

3 From the **Roles** Web page, select the check box beside the custom role or roles to delete.

The **Delete Roles** Web page appears with the selected roles for deletion, as shown in Figure 43 "Delete Roles Web page" (page 104).

Figure 43
Delete Roles Web page



Delete Roles

The following role(s) will be permanently deleted. All references to them will be removed from the system.

Roles: NewRole

To confirm deletion of the listed role(s), click Delete below.

4 Click **Confirm** to proceed with the deletion or **Cancel** to cancel the deletion.

—End—

Sessions

When the user clicks the Sessions link in the Security branch of the ECM navigator, the Active Sessions Web page appears. From the Active Sessions Web page, a security administrator can review user session information and terminate user sessions. With the appropriate permissions, a security administrator can view the session information for any user who is currently logged on.

View active sessions

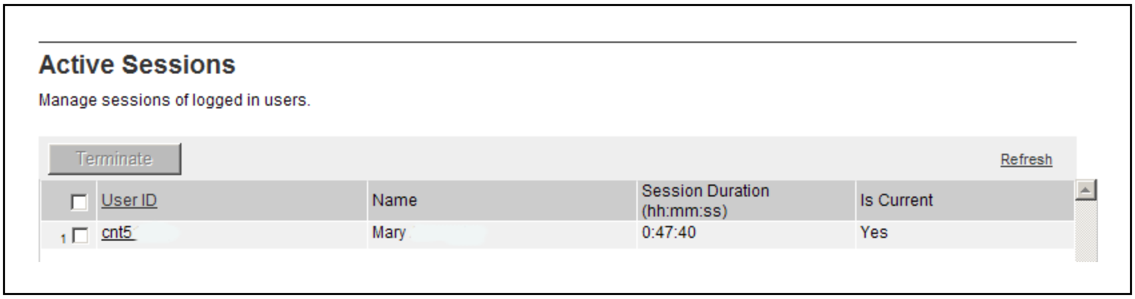
Security administrators can see all users who are currently logged on to ECM and view the session time for the user.

Use the steps in Procedure 50 "Viewing active sessions" (page 104) to view the current sessions in ECM.

Procedure 50
Viewing active sessions

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Sessions**. The **Active Sessions** Web page appears, as shown in Figure 44 "Active Sessions Web page" (page 105). The sessions are sorted in the **User ID** column.

Figure 44
Active Sessions Web page



Active Sessions

Manage sessions of logged in users.

	☐ User ID	Name	Session Duration (hh:mm:ss)	Is Current
1	☐ cnt5	Mary	0:47:40	Yes

—End—

Terminate SSO sessions

Use the steps in Procedure 51 "Terminating SSO sessions" (page 105) to terminate selected SSO sessions in ECM.

Procedure 51
Terminating SSO sessions

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** > **Sessions**. The **Active Sessions** Web page appears, as shown in Figure 44 "Active Sessions Web page" (page 105).
3	Select the required sessions to terminate.
4	Click **terminate**.

ATTENTION
A user cannot select a current session for termination.

Verify that the selected sessions are deleted from the current sessions table and that the administrators with terminated sessions are required to log on again.

—End—

Policies

When the user clicks the Policies link in the Security branch of the ECM navigator, the Policies Web page appears. From the Policies Web page, a security administrator can configure the authentication scheme, the authentication servers, and the password policies for ECM. A security administrator can also edit the ECM login banner message.

Review security policies

Use the steps in Procedure 52 "Reviewing security policies" (page 106) to review the currently configured security policies within the ECM.

Procedure 52
Reviewing security policies

Step **Action**

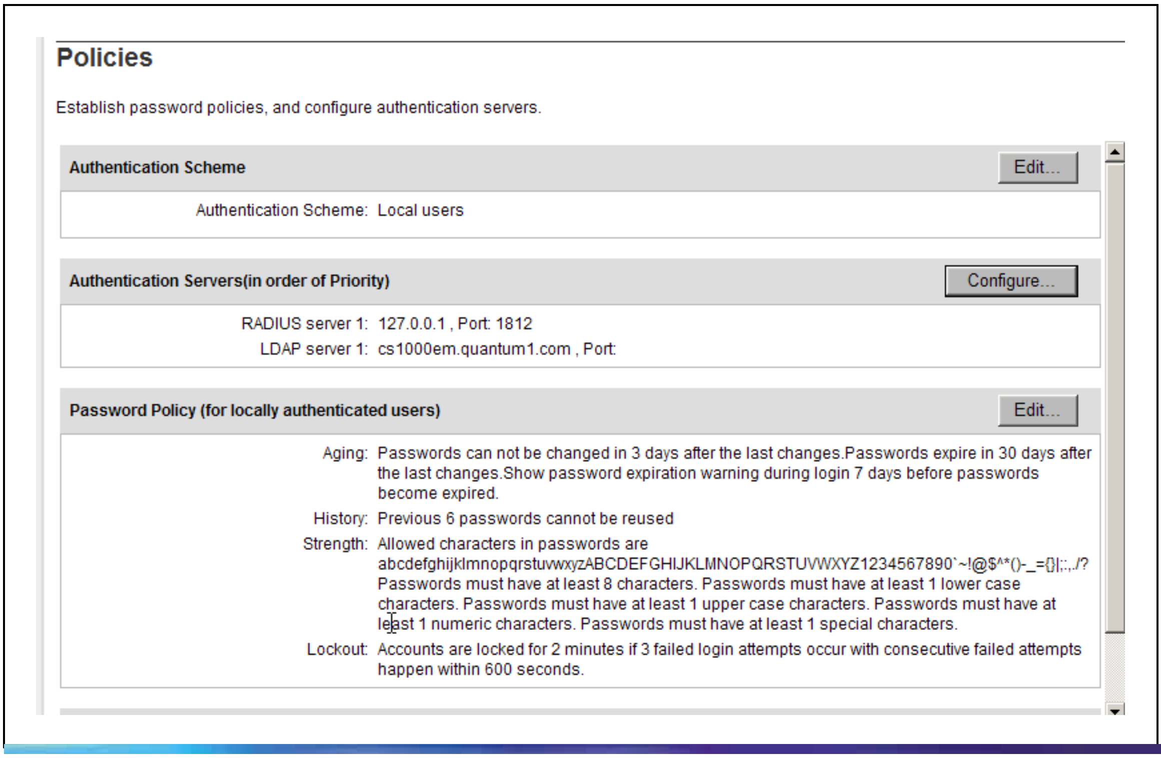
1 Log on to the ECM framework as a security administrator.

2 From the navigation pane, click **Security** > **Policies**.

The **Policies** Web page appears, as shown in Figure 45 "Policies Web page" (page 106).

3 From the **Policies** Web page, review the policy settings currently in ECM.

Figure 45
Policies Web page



Policies

Establish password policies, and configure authentication servers.

Authentication Scheme

Authentication Scheme: Local users

Authentication Servers(in order of Priority)

RADIUS server 1: 127.0.0.1 , Port: 1812
LDAP server 1: cs1000em.quantum1.com , Port:

Password Policy (for locally authenticated users)

Aging: Passwords can not be changed in 3 days after the last changes.Passwords expire in 30 days after the last changes.Show password expiration warning during login 7 days before passwords become expired.

History: Previous 6 passwords cannot be reused

Strength: Allowed characters in passwords are abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890`~!@$^*()-_={}|;:,./? Passwords must have at least 8 characters. Passwords must have at least 1 lower case characters. Passwords must have at least 1 upper case characters. Passwords must have at least 1 numeric characters. Passwords must have at least 1 special characters.

Lockout: Accounts are locked for 2 minutes if 3 failed login attempts occur with consecutive failed attempts happen within 600 seconds.

—End—

Edit the authentication scheme

Use the steps in Procedure 53 "Editing the authentication scheme" (page 107) to edit the authentication scheme. ECM supports up to three authentication authorities:

- local users
- external RADIUS users
- external LDAP users

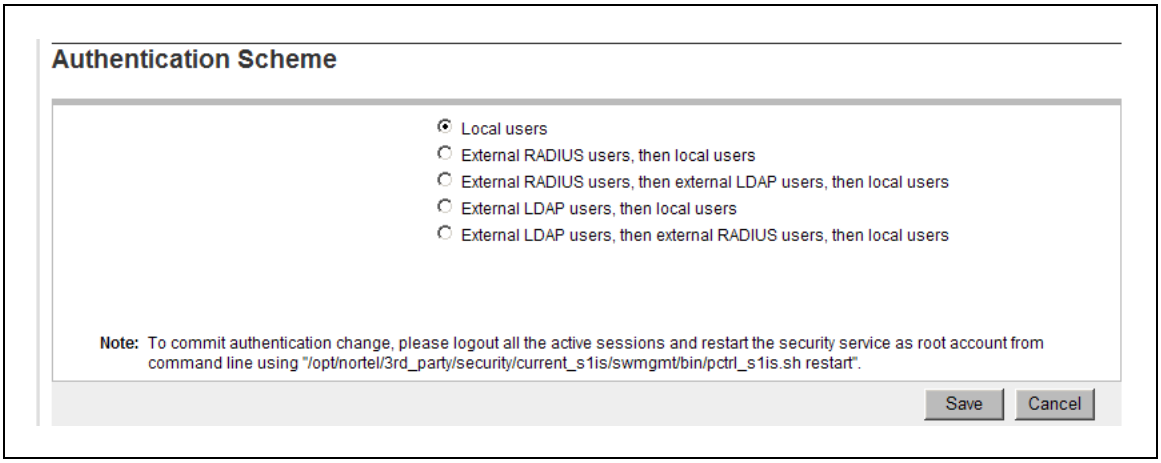
The authentication scheme policy determines the order that the three authentication authorities are used. The supported orders in ECM are as follows:

- local users (default)
- external RADIUS users then local users
- external LDAP users then local users
- external LDAP users, then external RADIUS users, then local users.
- external RADIUS users, then external LDAP users, then local users.

Procedure 53
Editing the authentication scheme

Step	Action
1	Log on to the ECM framework as a security administrator.
2	In the navigation pane, click **Security** > **Policies**. The **Policies** Web page appears, as shown in Figure 45 "Policies Web page" (page 106).
3	From the **Policies** Web page, in the **Authentication Scheme** section, click **Edit**. The **Authentication Scheme** Web page appears, as shown in Figure 46 "Authentication Scheme Web page" (page 108).

Figure 46
Authentication Scheme Web page



Authentication Scheme

● Local users
○ External RADIUS users, then local users
○ External RADIUS users, then external LDAP users, then local users
○ External LDAP users, then local users
○ External LDAP users, then external RADIUS users, then local users

Note: To commit authentication change, please logout all the active sessions and restart the security service as root account from command line using "/opt/nortel/3rd_party/security/current_s1is/swmgmt/bin/pctrl_s1is.sh restart".

4 Select the required authentication scheme, and click **Save**.

—End—

Configure the authentication servers

When the target LDAP server is not Microsoft Active Directory, the external user must have the uid attribute mapped to their login name. When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the login name that makes the cn attribute of the external users the same as the login name.

The TCP port that is used for the external LDAP server and UDP port used for the external RADIUS server must be open in the Linux iptables firewall on both the primary security service and back up primary security service. To check the status of the iptables rules, use "service iptables status."

Configure the LDAP authentication server

Use the steps in Procedure 54 "Configuring the LDAP authentication server" (page 108) to complete the required information for the LDAP authentication server.

Procedure 54
Configuring the LDAP authentication server

Step	Action
1	Log on to the ECM framework as a security administrator.
2	In the navigation pane, click **Security** > **Policies**.

The **Policies** Web page appears, as shown in Figure 45 "Policies Web page" (page 106).

3 From the **Policies** Web page in the **Authentication Servers** section, click **Configure**.

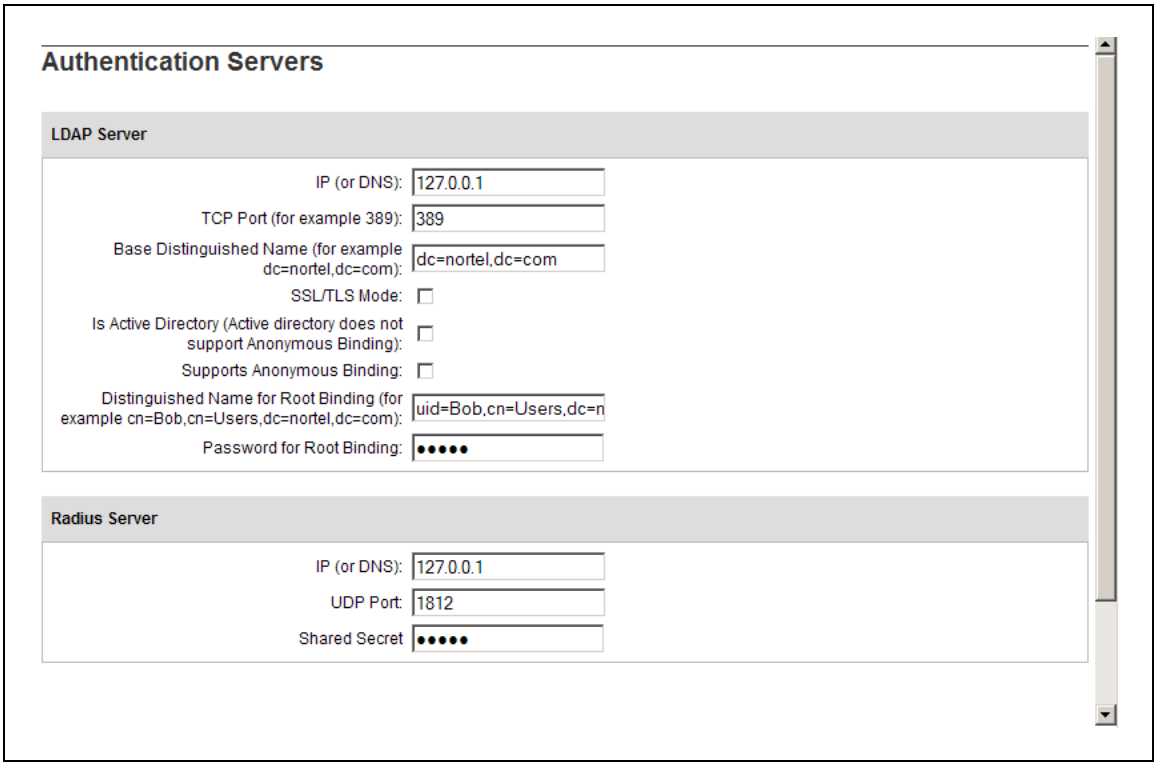
The **Authentication Servers** Web page appears, as shown in Figure 47 "Authentication Servers Web page" (page 110).

4 In the **LDAP Server**, enter the following information:

- In the **IP (or DNS)** field, type the IP address or DNS name of the LDAP server.
- In the **TC Port** field, type the TC port number of the LDAP server.
- In the **Base Distinguished Name** field, enter the base DN of the LDAP server.
- Select **SSL/TLS Mode** if the LDAP server supports SSL/TLS connections.
- Select **Is Active Directory** if active directory does not support anonymous binding.
- Select **Supports Anonymous Binding** if supported.
- In the **Distinguished Name for Root Binding** field, type the distinguished name for the root binding.
- In the **Password** field, type the password for the root binding.

5 Click **Save**.

Figure 47
Authentication Servers Web page



Authentication Servers

LDAP Server

IP (or DNS): 127.0.0.1

TCP Port (for example 389): 389

Base Distinguished Name (for example dc=nortel,dc=com): dc=nortel,dc=com

SSL/TLS Mode: □

Is Active Directory (Active directory does not support Anonymous Binding): □

Supports Anonymous Binding: □

Distinguished Name for Root Binding (for example cn=Bob,cn=Users,dc=nortel,dc=com): uid=Bob,cn=Users,dc=n

Password for Root Binding: ●●●●●

Radius Server

IP (or DNS): 127.0.0.1

UDP Port: 1812

Shared Secret ●●●●●

> **ATTENTION**
> Ensure the Linux iptable firewall setting on both the primary and backup security service allows the TCP port as source port.

—End—

Configure the RADIUS authentication server

Use the steps in Procedure 55 "Configuring the RADIUS authentication server" (page 110) to complete the required information for the RADIUS authentication server.

Procedure 55
Configuring the RADIUS authentication server

Step	Action
1	Log on to the ECM framework as a security administrator.
2	In the navigation pane, click **Security** > **Policies** as shown in Figure 45 "Policies Web page" (page 106).

The **Policies** Web page appears.

3 From the **Policies** Web page in the **Authentication Servers** section, click **Configure**.

The **Authentication Servers** Web page appears, as shown in Figure 47 "Authentication Servers Web page" (page 110).

4 In the **RADIUS Server**, enter the following information:

- In the **IP (or DNS)** field, type the IP address or DNS name of the primary RADIUS server.
- In the **UDP Port** field, type the UDP port number of the primary RADIUS server.
- In the **Shared Secret** field, type the shared secret of the RADIUS server.

5 Click **Save**.

> **ATTENTION**
> Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as source port.

—End—

Edit local account password policies

Use the steps in Procedure 56 "Editing password policies" (page 111) to configure the local account password policies including, aging, history, strength, and lockout password policies in ECM according to business requirements.

Procedure 56
Editing password policies

Step **Action**

1 Log on to the ECM framework as a security administrator.

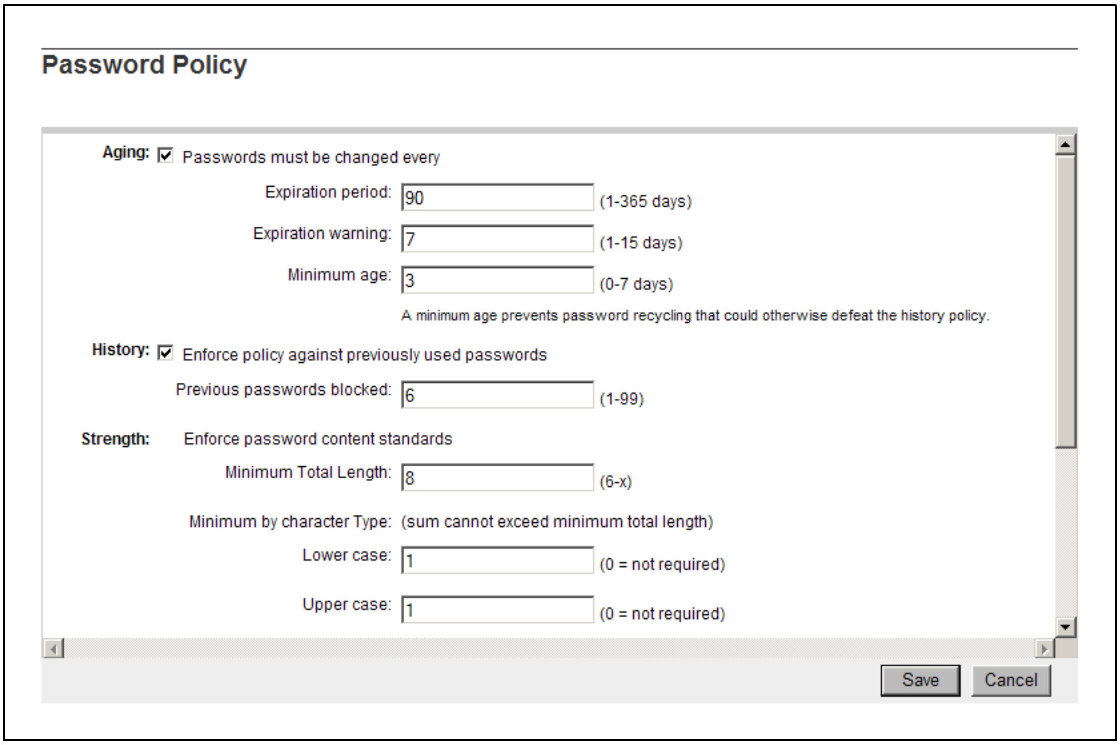
2 In the navigation pane, click **Security** > **Policies**.

The **Policies** Web page appears, as shown in Figure 45 "Policies Web page" (page 106).

3 From the **Policies** Web page in the **Password Policy** section, click **Edit**, as shown in Figure 45 "Policies Web page" (page 106).

The **Password Policy** Web page appears, as shown in Figure 48 "Password Policy Web page" (page 112).

Figure 48
Password Policy Web page



Password Policy

Aging: ☑ Passwords must be changed every

Expiration period: 90 (1-365 days)

Expiration warning: 7 (1-15 days)

Minimum age: 3 (0-7 days)

A minimum age prevents password recycling that could otherwise defeat the history policy.

History: ☑ Enforce policy against previously used passwords

Previous passwords blocked: 6 (1-99)

Strength: Enforce password content standards

Minimum Total Length: 8 (6-x)

Minimum by character Type: (sum cannot exceed minimum total length)

Lower case: 1 (0 = not required)

Upper case: 1 (0 = not required)

4 In the **Aging** section, perform the following actions:

- Select **Aging**.
- In the **Expiration period** field, type a number from 1 to 365 for the maximum allowable days for the password. The default value is 90.
- In the **Expiration warning** field, type a number from 1 to 15 to send a warning message to a user that the password is about to expire. The default value is 7.
- In the **Minimum age** field, type a number between 0 to 7 for the minimum allowable days for password age. The default value is 3.

  Ensure that the number for the expiration period is higher than the minimum password age number.

ATTENTION

All passwords can expire. If an administrator's password expires, the administrator can reset the password through the Command Line Interface (CLI), as shown in Procedure 3 "Resetting a user password from the CLI" (page 39).

5 In the **History** section, perform the following actions:

- Select **History**.
- In the **Previous passwords blocked** field, type a number from 1 to 99 for the number of passwords to remember in history. The default value is 6.

6 In the **Strength** section, perform the following actions:

- In the **Minimum Total Length** field, type a number for the minimum number of total characters for the password. The minimum range is 6 to x. The default value is 8.

  In the **Minimum by character Type** fields, do the following:

- In the **Lower case** field, type the minimum number of lowercase characters for the password 0 to x. The default value is 1.
- In the **Upper case** field, type the minimum number of uppercase characters for the password from 0 to x. The default value is 1.
- In the **Numeric case** field, type the minimum number of numeric characters for the password from 0 to x. The default value is 1.
- In the **Special case** field, type the minimum number of special characters for the password from 0 to x. The default value is 1.

7 In the **Lockout** section, perform the following actions:

- Select **Lockout**.
- In the **Consecutive Invalid Login Attempts** field, type a number for failed attempts from 1 to x. The default value is 5.
- In the **Interval for Consecutive Invalid Login Attempts** field, type the interval in number of seconds from 0 to x for consecutive invalid logon attempts. The default is 600 seconds.
- In the **Lockout Time** field, type the number of minutes from 0 to x until the account is unlocked. The default is two minutes.

ATTENTION

An invalid logon message appears for the following scenarios:

- A user logs in with a disabled account.
- The user's password is invalid.
- The user exceeds the maximum number of log on attempts.
- The user's password expired.

For each scenario, the system responds with a message that invalid login credentials were used. The user must contact the security administrator for additional information.

ATTENTION

A user can log on successfully with a valid user name and password when the required time for failed log on attempts is reached.

The system sends a warning message when a password is about to expire. The user must change the password.

8 Click **Save**.

—End—

Edit the login warning banner

ECM provides a customizable login banner that appears when a user logs on to the system. The customizable banner is intended for use by customers that have security policies that require network equipment to display a specific message to users when they log on. The default login warning banner message is shown in Table 12 "Default Login warning message" (page 114)

Table 12
Default Login warning message

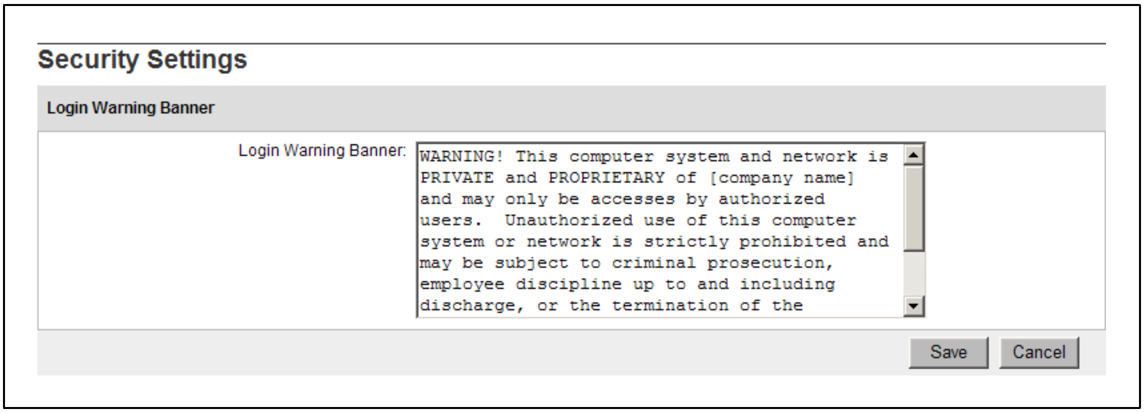
WARNING! This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accesses by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

Use the steps in Procedure 57 "Editing the login warning banner" (page 115) to customize the message for the login warning banner in ECM.

Procedure 57
Editing the login warning banner

Step	Action
1	Log on to the ECM framework as a security administrator.
2	In the navigation pane, click **Security** > **Policies**. The **Policies** Web page appears, as shown in Figure 45 "Policies Web page" (page 106).
3	From the **Policies** Web page in the **Security Settings** section, click **Edit**. The **Login Warning Banner Web** page appears, as shown in Figure 49 "Login Warning Banner Web page" (page 115)

Figure 49
Login Warning Banner Web page



Security Settings

Login Warning Banner

Login Warning Banner:

```
WARNING! This computer system and network is
PRIVATE and PROPRIETARY of [company name]
and may only be accesses by authorized
users.  Unauthorized use of this computer
system or network is strictly prohibited and
may be subject to criminal prosecution,
employee discipline up to and including
discharge, or the termination of the
```

Step	Action
4	In the **Login Warning Banner** text area, edit the text as required.
5	Click **Save**.

—End—

Tools

Contents

This chapter contains information on the following topics:

The Tools branch in the Enterprise Common Manager (ECM) navigation pane contains links to the following tools:

- Logs
- SNMP

Logs

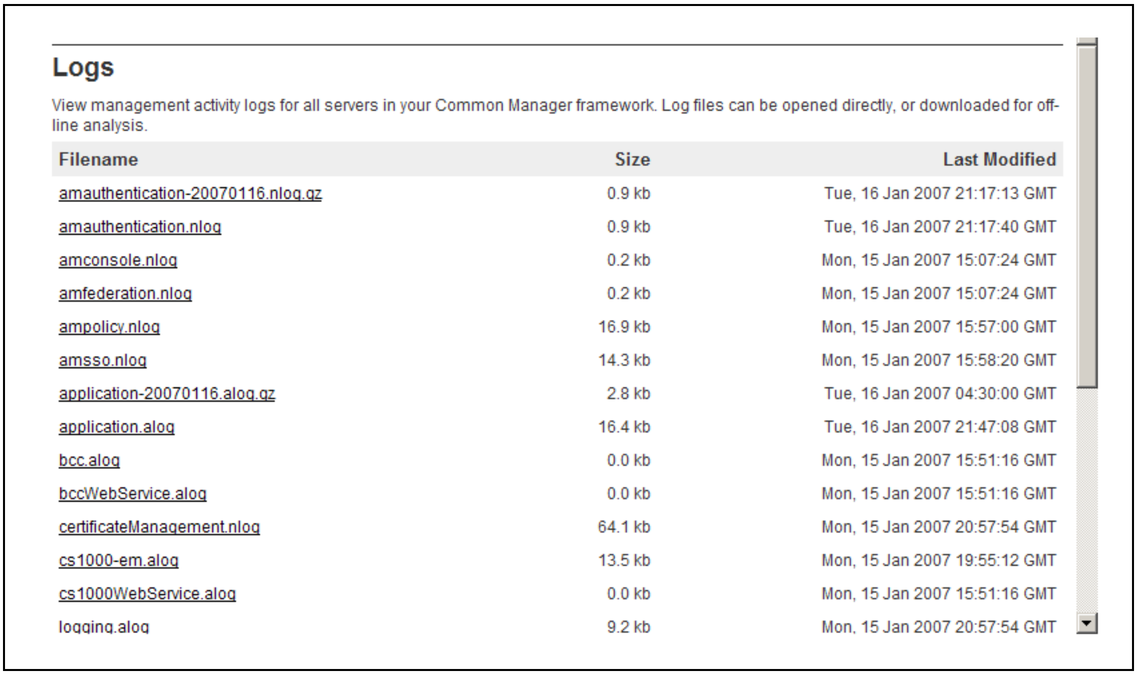
When the user clicks the Logs link in the Tools branch of the ECM navigator, the Logs Web page appears. From the Logs Web page, a security administrator can review or download log files.

Use the steps in Procedure 58 "Reviewing log files" (page 117) to review management activity logs in the current or a new Web browser window or to download a log file.

Procedure 58
Reviewing log files

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Tools** > **Logs**. The directory list for recorded logs Web page appears, as shown in Figure 50 "Directory Listing For logs Web page" (page 118).

Figure 50
Directory Listing For logs Web page



Logs

View management activity logs for all servers in your Common Manager framework. Log files can be opened directly, or downloaded for off-line analysis.

Filename	Size	Last Modified
amauthentication-20070116.nlog.gz	0.9 kb	Tue, 16 Jan 2007 21:17:13 GMT
amauthentication.nlog	0.9 kb	Tue, 16 Jan 2007 21:17:40 GMT
amconsole.nlog	0.2 kb	Mon, 15 Jan 2007 15:07:24 GMT
amfederation.nlog	0.2 kb	Mon, 15 Jan 2007 15:07:24 GMT
ampolicy.nlog	16.9 kb	Mon, 15 Jan 2007 15:57:00 GMT
amsso.nlog	14.3 kb	Mon, 15 Jan 2007 15:58:20 GMT
application-20070116.alog.gz	2.8 kb	Tue, 16 Jan 2007 04:30:00 GMT
application.alog	16.4 kb	Tue, 16 Jan 2007 21:47:08 GMT
bcc.alog	0.0 kb	Mon, 15 Jan 2007 15:51:16 GMT
bccWebService.alog	0.0 kb	Mon, 15 Jan 2007 15:51:16 GMT
certificateManagement.nlog	64.1 kb	Mon, 15 Jan 2007 20:57:54 GMT
cs1000-em.alog	13.5 kb	Mon, 15 Jan 2007 19:55:12 GMT
cs1000WebService.alog	0.0 kb	Mon, 15 Jan 2007 15:51:16 GMT
logging.alog	9.2 kb	Mon, 15 Jan 2007 20:57:54 GMT

3 Click a **Filename** to review the file information in the current window.

To open a log file in a new browser window, right-click the name of a log file and select **Open in new window**.

To download a log file, right-click the name of a log file and select **Save target as**. Select a location on the computer to save the log file.

—End—

SNMP

When the user clicks the SNMP link in the Tools branch of the ECM navigator, the SNMP Web page appears. From the SNMP Web page, a security administrator can view, edit, enable, or disable SNMP for ECM.

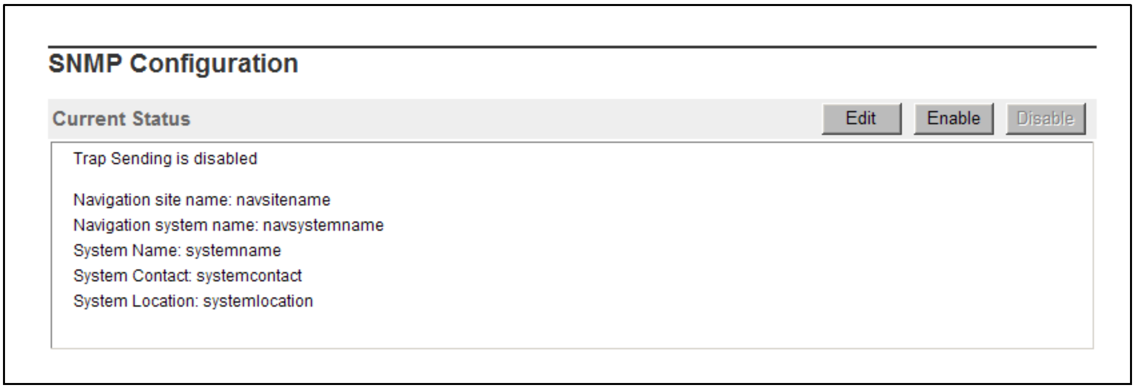
View the status of SNMP

Use the steps in Procedure 59 "Viewing the status of SNMP" (page 119) to view the current status for SNMP.

Procedure 59
Viewing the status of SNMP

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Tools** > **Snmp**. The **SNMP Configuration** Web page appears, as shown in Figure 51 "SNMP Web page" (page 119).

Figure 51
SNMP Web page



SNMP Configuration

Trap Sending is disabled

Navigation site name: navsitename
Navigation system name: navsystemname
System Name: systemname
System Contact: systemcontact
System Location: systemlocation

The **SNMP Configuration** Web page displays the current SNMP status information.

—End—

Modify the SNMP configuration

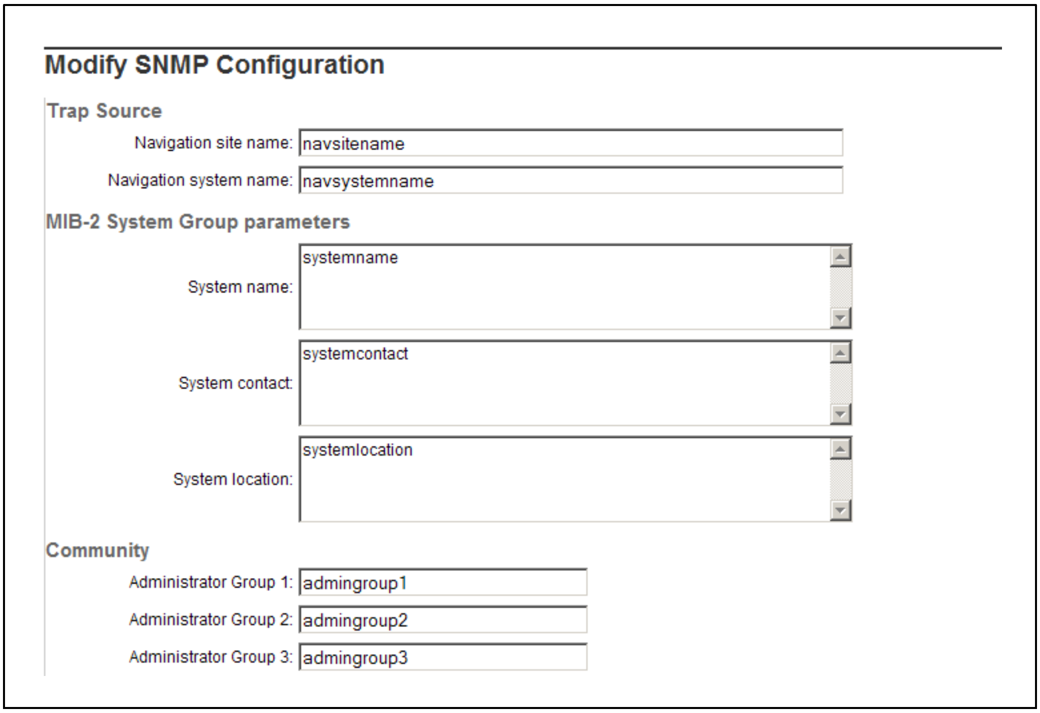
Use the steps in Procedure 60 "Modifying the SNMP configuration" (page 119) to modify the SNMP configuration.

Procedure 60
Modifying the SNMP configuration

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Tools** > **Snmp**. The SNMP Configuration Web page appears, as shown in Figure 51 "SNMP Web page" (page 119).
3	Click **Edit**.

The **Modify SNMP Configuration** Web page appears, as shown in Figure 52 "Modify SNMP Configuration Web page" (page 120).

Figure 52
Modify SNMP Configuration Web page



Modify SNMP Configuration

Trap Source

Navigation site name: navsitename

Navigation system name: navsystemname

MIB-2 System Group parameters

System name: systemname

System contact: systemcontact

System location: systemlocation

Community

Administrator Group 1: admingroup1

Administrator Group 2: admingroup2

Administrator Group 3: admingroup3

4 From the **Modify SNMP Configuration** Web page, edit the information for SNMP as follows:

- For **Trap Source**, edit the following fields as required:
  - — System name
  - — System contact
  - — System location

- For **MIB-2 System Group parameters**, edit the following fields as required:
  - — System name
  - — System contact
  - — System location

- For **Community**, edit the following fields as required:
  - — Administrator Group 1
  - — Administrator Group 2
  - — Administrator Group 3

- System management read
- System management read/write
- Trap community

- For **Trap Destination**, edit the following fields as required:
  - IPAddress1
  - IPAddress2
  - IPAddress3
  - IPAddress4
  - IPAddress5
  - IPAddress6
  - IPAddress7
  - IPAddress8

5 Click **Save**.

—End—

Enable or disable trap sending

Use the steps in Procedure 61 "Enabling or disabling trap sending" (page 121) to enable or disable trap sending for SNMP configuration in ECM.

Procedure 61

Enabling or disabling trap sending

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Tools** > **Snmp**. The SNMP Configuration Web page appears, as shown in Figure 51 "SNMP Web page" (page 119).
3	From the SNMP Web page, click **Enable Trap** or **Disable Trap** to enable or disable trap sending.

—End—

Upgrade

This chapter contains the following tasks:

- "Upgrade the ECM primary and backup security service on a Linux server" (page 123)
- "Upgrade the ECM security member server" (page 124)
- "Reinstall the ECM security service applications on a Linux server" (page 124)

Upgrade the ECM primary and backup security service on a Linux server

When an application is upgraded, any existing data is backed up into a temporary directory (/admin/nortel/ isclient/DDMMYYYY.tar) and is restored after the upgrade. The tar file name is based on the current date in the DDMMYYYY format. The tar file is removed after upgrade.

The config.xml of the ECM isclient application contains the reference to the scripts used for backup and restore. The appinstall master script triggers the backup and restore scripts for isclient application during update.

Use the steps in Procedure 62 "Upgrading the ECM primary and backup security service on a Linux server" (page 123) to upgrade the current ECM primary and backup security service on a Linux server.

Procedure 62
Upgrading the ECM primary and backup security service on a Linux server

Step	Action
1	Insert the new application CD in the CD drive of the Linux server.
2	Select **Upgrade existing applications on the Linux server**. The appinstall master script performs the following actions: • starts the backup script for the isclient application when isclient config.xml is complete • uninstalls the current applications

- starts the installation from the new application CD
- starts the configuration script for each of the applications
- starts the restore script

ATTENTION
When configuring the private security authority, choose not to configure the private CA.

The appinstall script starts the restore script for the isclient application when the isclient config.xml is complete.

—End—

Upgrade the ECM security member server

Use the steps in Procedure 63 "Upgrading the ECM security member server" (page 124) to upgrade the current ECM security member server.

Procedure 63
Upgrading the ECM security member server

Step Action

1 Insert the new application CD in the CD drive of the Linux server.

2 Select **Upgrade existing applications on the Linux server**.

The appinstall master script performs the following actions:

- starts the backup script
- uninstalls the current applications
- starts the installation from the new application CD
- starts the configuration script for each of the applications
- starts the restore script

—End—

Reinstall the ECM security service applications on a Linux server

Use the steps in Procedure 64 "Reinstalling the ECM security service applications on a Linux server" (page 125) to reinstall the ECM security service applications on a Linux server.

Procedure 64
Reinstalling the ECM security service applications on a Linux server

Step	Action
1	Insert the new application CD in the CD drive of the Linux server.
2	Select **Reinstall applications on the Linux server**. The appinstall master script does the following: • uninstalls the current applications • starts the installation from the new application CD • starts the configuration script for each of the applications

—End—

Backup and restore

This chapter contains the following topics:

Enterprise Common Manager (ECM) supports backup and restore for the following data types:

- data from the certificate management module and the private certificate authority (CA) module under /etc/opt/ssl
- data from security service

Backup script

Perform backups for the following information:

- private certificate authority, application server certificates and keys, trusted/untrusted certificate authority, and configuration files such as Web Secure Socket Layer (SSL) and Session Initiation Protocol (SIP) Transport Layer Security (TLS)
- security core
- security client PAM and NSSwitch

To perform a backup procedure, a user must log on as the root user and run the following script:

```
/opt/nortel/isclient/backup_ss.sh -path <path>
```

Restore script

To perform a restore, a user must log on as the root user and run the following script:

```
/opt/nortel/isclient/restore_ss.sh -path <path>
```

ATTENTION
To perform a backup or restore, a user must have previously created backup files.

Back up and restore in high availability mode

A user cannot restore high availability that is replicated between the primary security service and backup security service.

Before a user can restore files, they must log on as the root user to the primary security service and run the following script:

```
/opt/nortel/isclient/setup_ssha.sh deconfig
```

After a restore on either the primary security service or the backup security service, log on as the root user to the primary security service and run the following script:

```
/opt/nortel/isclient/setup_ssha.sh config
```

Back up from one server and restore to another server

Support exists to backup from one server and to restore to another server if the new server uses the same Fully Qualified Domain Name (FQDN) and IP address as the old server and it is not running the primary security service.

Back up during an upgrade

During an application upgrade, existing data is backed up to a temporary directory (/admin/nortel/ isclient/DDMMYYYY.tar) and restored after the upgrade. The tar file name is based on the current date in the DDMMYYYY format and the file is removed after the upgrade.

Backup and restore directories

Backups are stored in the following directories:

- /etc/opt/nortel/ssl
- /etc/ssh
- /root/.ssh
- /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

Log files in the following directories are backed up and restored:

- /opt/nortel/logs/3rd_party/netscape
- /opt/nortel/logs/3rd_party/security/s1is
- /opt/nortel/logs/applications/security

Do not use the following locations when restoring data:

- /etc/opt/nortel/ssl
- /etc/ssh
- /root/.ssh
- /opt/nortel/applications/security
- /opt/nortel/config/applications/security
- /opt/nortel/data/applications/security
- /opt/nortel/logs/applications/security

Appendix A
Modify the IP addresses for installed servers

Modify the IP addresses for the installed servers and the FQDN for the member server

Use these procedures to change the TLAN (eth1) and ELAN (eth0) network interface IP addresses for the primary, backup, and member servers and to change the Fully Qualified Domain Name (FQDN) of the security member server.

Modify the TLAN (eth1) network interface IP address of the primary, backup, or member server

Use the steps in Procedure 65 "Modifying the TLAN (eth1) network interface IP address of the primary, backup, or member server" (page 131) to modify the TLAN (eth1) network interface IP address by changing the mapping for FQDN, in the DNS server, or in the PC Web client.`/etc/hosts`.

Procedure 65

Modifying the TLAN (eth1) network interface IP address of the primary, backup, or member server

Step	Action
1	Log on with account Nortel.
2	At the prompt, enter `su` to switch to superuser mode.
3	At the prompt, enter the root password.
4	Change the IP address of eth1 through baseparamsconfig to root.
5	Enter the new IP address for FQDN mapping in `/etc/hosts`.
6	Enter the FQDN mapping in the DNS server or in the PC Web client `C:\WINNT\system32\drivers\etc\hosts`.

ATTENTION
Change the `/etc/hosts` in all the Linux servers if the DNS server is not used.

7 With a root account, perform the following tasks:

- For the primary server run
  - — `ssh newTLANIpAddress`. The system responds with the following:

```
[root@otmhp3~]# ssh 47.11.151.69
The authenticity of host
'47.11.151.69(47.11.151.69)' can't be
established.
RSA key fingerprint is
78:0d:1d:ec:1c:a0:b1:c3:5d:4d:3f:06:bc:be:7b:49.
Are you sure you want to continue connecting
(yes/no)?
```

    Type `Yes` and press **Enter**.

- For the backup or member server run
  - — `/opt/nortel/linuxTrustMgmt/setupNonCA.sh`

ATTENTION
Change the `/etc/hosts` in all the Linux servers if the DNS server is not used.

—End—

Modify the ELAN (eth0) network interface IP address of the primary, backup, and member servers

To modify the ELAN (eth0) network interface IP address of the primary, backup, and member servers, change the IP address of eth0 through ifconfig to root.

Modify the FQDN of the security member server

Use the steps in Procedure 66 "Modifying the FQDN of the security member server" (page 133) to change the FQDN of the security member server by changing the host name and FQDN, and by changing the FQDN mapping in the DNS server or PC Web client.

Procedure 66
Modifying the FQDN of the security member server

Step	Action
1	Change the host name and FQDN of the member server to root.
2	Enter the host name for the FQDN mapping in `/etc/hosts`.
3	Enter the FQDN mapping in the DNS server or in the PC Web client `C:\WINNT\system32\drivers\etc\hosts`.

ATTENTION
Change the `/etc/hosts` in all the Linux servers if the DNS server is not used.

Step	Action
4	Recreate the WEB SSL and SIP TLS server certificate from the primary security service with the new FQDN.

—End—

Appendix B
Linux root account Command Line Interface commands

Table 13 "Linux root account CLI commands" (page 135) describes the Command Line Interface (CLI) and debug commands that ECM uses. For each of the CLI commands, log on to the CLI with a root account and run the CLI command script.

Table 13
Linux root account CLI commands

Action	CLI command script
Start the Sun Access Manager LDAP server.	/opt/nortel/3rd_party/netscape/current_nds/swmgmt/bin/pctrl_nds.sh start
Stop the Sun Access Manager LDAP server.	/opt/nortel/3rd_party/netscape/current_nds/swmgmt/bin/pctrl_nds.sh stop
Restart the Sun Access Manager LDAP server.	/opt/nortel/3rd_party/netscape/current_nds/swmgmt/bin/pctrl_nds.sh restart
View the status for the Sun Access Manager LDAP server.	/opt/nortel/3rd_party/netscape/current_nds/swmgmt/bin/pctrl_nds.sh status
Start the Sun Access Manager Web server.	/opt/nortel/3rd_party/security/ current_s1is/swmgmt/ bin/pctrl_s1is.sh start
Stop the Sun Access Manager Web server.	/opt/nortel/3rd_party/security/ current_s1is/swmgmt/ bin/pctrl_s1is.sh stop
Restart the Sun Access Manager Web server.	/opt/nortel/3rd_party/security/ current_s1is/swmgmt/ bin/pctrl_s1is.sh restart
View the status for the Sun Access Manager Web server.	/opt/nortel/3rd_party/security/ current_s1is/swmgmt/ bin/pctrl_s1is.sh status
Start the ECM JBoss Web Server.	service jbossd start
Stop the ECM JBoss Web Server.	service jbossd stop
Restart the ECM JBoss Web Server.	service jbossd restart
View the status for the ECM JBoss Web Server.	service jbossd status

Action	CLI command script
Print the fingerprint for the RSA/DSA key that is stored in the keyFile.	/opt/nortel/privateCA/ showFingerprint.sh [key-FileName]
View the IP address to host key mapping of the servers in the security domain.	cat /root/.ssh/known_hosts
View the public key trusted by the Linux root account.	cat /root/.ssh/authorized_keys
From the primary security server, view the member servers in the security domain and the applications installed on each member server.	cat /etc/opt/nortel/isclient/member_register
View the primary security server Fully Qualified Domain Name (FQDN).	cat /etc/opt/nortel/isclient/fqdn.primary.hostname
From the member server or backup security server, view the primary security server TLAN network interface IP address.	cat /etc/ opt/nortel/isclient/tlan.primary.hostname
From the member server or backup security serve, register the Linux server to the primary security server. This command executes automatically during installation. This command performs the following actions: • registers the trust between the member server and the primary security server • generates the default Web SSL certificate for the member server • synchronizes the system account passwords from the primary security server Execute this command manually only for debug purposes.	/opt/nortel/linuxTrustMgmt/setupNonCA.sh
Back up the ECM security data.	/opt/nortel/isclient/backup_ss.sh
Restore the ECM security data.	/opt/nortel/isclient/restore_ss.sh
Configure the high availability between the primary security server and the backup security server.	/opt/nortel/isclient/setup_ssha.sh config
Clear the high availability between the primary security server and the backup security server.	/opt/nortel/isclient/setup_ssha.sh deconfig
Change or synchronize system account passwords.	/opt/nortel/isclient/change_syspasswd.sh
Reset an account from the CLI.	/opt/nortel/applications/security/current_isclient/bin/is_passwd.sh

Action	CLI command script
Debug in the nss_saml module.	/opt/nortel/applications/security/current_nsssaml/bin/ nssquery
View the error log for the Sun Access Manger Web server.	cat /opt/sun/webserver/https-oamplatform/logs/errors

Appendix C
Example of a least privilege algorithm

The following is an example of a least privilege algorithm:

Tom is assigned two roles as PowerUser and ReadOnly. A managed element nrsAnytown has two permissions that are nrsmAdmin and nrsmMonitor.

The role of PowerUser is granted to nrsmAdmin and nrsmMonitor.

The role of ReadOnly is denied to nrsmAdmin but is granted to nrsmMonitor.

When Tom attempts to access nrsAnytown, ECM applies the least privilege algorithm that grants Tom nrsmMonitor and denies Tom nrsmAdmin.

Table 14 "Least privilege algorithm" (page 139) shows the least privilege algorithm for Tom.

Table 14
Least privilege algorithm

User Permission	nrsmAdmin	nrsmMonitor
PowerUser	Granted	Granted
ReadOnly	Denied	Denied
Tom	Denied	Granted

Appendix D
Example of role- and instance-based access control in CS 1000 systems

The following scenario is an example of role- and instance-based access control for Communication Server (CS) 1000 systems.

ABC company uses CS 1000 VoIP solutions for its internal voice network.

The company has two CS 1000 systems in Anytown:

- CS1000_Mall
- CS1000_Hospital

The company also has two CS 1000 systems in Anycity:

- CS1000_College
- CS1000_HighSchool

The company's access control policies are as follows:

- Only the dedicated security administrator of the company can add, delete, or edit accounts in all the CS 1000 systems.
- The software upgrade of all the CS 1000 systems are out-sourced to a Nortel distributor company. Only authorized personnel from the distributor company can perform tasks such as patching and upgrading for the CS 1000 systems.
- The IP Phone location information for E911 is maintained by a third party as an E911 application. Only the E911 application is authorized to add, delete, or edit E911 information within the CS 1000 systems.
- The maintenance work for the CS 1000 systems of Anytown and Anycity must have a different administrator assigned to each system.

The following two steps are required to implement the access control policies for the company in the security framework:

- The company must assign permissions for roles for the CS 1000 systems, create new roles if necessary, and assign administrators to these roles. The roles are as follows:
  - The built-in role SecurityAdministrator for the dedicated security administrator.
  - The built-in role Patcher for authorized personnel from the distributor company.
  - A custom role E911 is created for the E911 application.
  - The custom roles AnytownAdmin and AnycityAdmin are created for the different administrators assigned to the CS 1000 systems:
    - AnytownAdmin has UnRestrictedOamAccess to CS1000_Mall and CS1000_Hospital.
    - AnycityAdmin has UnRestrictedOamAccess to CS1000_College and CS1000_HighSchool.
- The company must assign administrators to roles.

Table 15 "Permission assignment for the roles in ABC company" (page 142) shows the permission assignment for the roles in ABC company.

Table 15
Permission assignment for the roles in ABC company

Role Name CS 1000 Name	CS1000_Mall	CS1000_ Hospital	CS1000_ College	CS1000_High School
SecurityAdministrator (built-in)	• UnRestrictedOamAccess • SecAdmin • Account Admin	• UnRestrictedOamAccess • SecAdmin • Account Admin	• UnRestricted OamAccess • SecAdmin • Account Admin	• UnRestricted OamAccess • SecAdmin • Account Admin
Patcher	• OamUser • Pdt1Access	• OamUser • Pdt1Access	• OamUser • Pdt1Access	• OamUser • Pdt1Access
E911	• Permission _E911	• Permission_ E911	• Permission_ E911	• Permission_ E911
AnytownAdmin	• UnRestrictedOamAccess	• UnRestrictedOamAccess		
AnyCityAdmin			• UnRestricted OamAccess	• UnRestricted OamAccess

ABC company has the following administrative staff:

- Steve is the security administrator and the administrator for the CS 1000 systems for Anytown.
- Bob is the technician from the distributor company.
- Danny is the administrator name used for the third-party E911 application to contact the CS 1000 systems.
- Jin is the administrator for the CS 1000 systems for Anycity.

Table 16 "ABC company administrator role assignments" (page 143) shows the administrator role assignments for ABC company.

Table 16
ABC company administrator role assignments

User/Role	Security Administrator	Patcher	E911	AnytownAdmin	AnycityAdmin
Steve	X			X	
Bob		X			
Danny			X		
Jin					X

As shown in Table 16 "ABC company administrator role assignments" (page 143), the user role and element permission mapping assignments meet the access control requirements for ABC company. The user role assignments are described as follows for ABC company.

- Only Steve can add, delete, or edit accounts in all the CS 1000 systems. Steve also performs the maintenance work of CS 1000 systems of Anytown.
- Bob from the distributor company can patch, upgrade, and perform related tasks for the CS 1000 systems.
- Account Danny can add, delete, or edit the E911 related information of the CS1000 systems.
- Jin performs the maintenance work of CS 1000 systems of Anycity.

Appendix E
Red Hat passthrough end user license agreement

WARNING
Do ***not*** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

This governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to the user ("Customer") a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the "Red Hat Software") is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component's source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer's rights under, or grant Customer rights that supersede, the license terms of any particular component. The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat's trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and “anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department’s Export Administration Regulations (“EAR”); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department’s Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. Copyright © 2003 Red Hat, Inc. All rights reserved. "Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Index

Nortel Communication Server 1000

Enterprise Common Manager Fundamentals

Publication: NN43001-116
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

To provide feedback or to report a problem with this document, go to www.nortel.com/documentfeedback.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.