Nortel Communication Server 1000

Enterprise Common Manager Fundamentals

Release: Release 5.5
Document Revision: 02.12

www.nortel.com

NN43001-116

Nortel Communication Server 1000
Release: Release 5.5
Publication: NN43001-116
Document release date: 26 November 2008

Sourced in Canada

Contents

New in this Release

The Enterprise Common Manager is issued to support Communication Server 1000 Release 5.5.

Navigation

Features

See the following sections for information about feature changes:

Management of multiple releases

For Release 5.5, ECM supports the management of multiple releases (5.0 and 5.5) for network elements. When network elements are upgraded, the CS 1000 elements in the ECM framework must be configured to launch the Release 5.5 management Web application.

Table 1 "Elements that can have multiple versions" (page 7) shows the elements that can have multiple versions in ECM.

Table 1
Elements that can have multiple versions

Element	Multiple versions
Element Manager	Yes
Basic Client Configuration	Yes
NRS Manager	Yes
Bookmark	No

Nortel recommends you perform a system-level backup of ECM before an upgrade. If you choose not to upgrade, you can delete and then create the elements for CS 1000 Release 5.5.

Configure Single Sign-On cookie domain

In Release 5.5 users can change the Single Sign-On (SSO) cookie domain. To configure the SSO cookie domain, see "Edit the SSO cookie domain" (page 126).

Additional enhancements

ECM supports the following additional enhancements for Release 5.5:

- Support for appending the logs of fast sync to centralized logging
- Validation for IP and FQDN properties in the ECM framework
- Modification for buttons in the Assigned Users Web page
- Highlighting for the selected node in the navigation tree

Other

See the following section for information about changes that are not feature-related:

Revision History

November 2008
Standard 02.12. This document is up-issued to reflect changes in section Security domain.

July 2008
Standard 02.11. This document is up-issued to reflect changes in Security management.

February 2008 Standard 02.10. This document is up-issued to reflect changes in technical content.

February 2008 Standard 02.09. This document is up-issued to reflect changes in technical content.

January 2008 Standard 02.08. This document is up-issued to reflect changes in technical content.

December 2007 Standard 02.07. This document is up-issued to reflect changes in technical content.

December 2007 Standard 02.06. This document is up-issued to reflect changes in technical content.

December 2007 Standard 02.05. This document is up-issued to support Communication Server 1000 Release 5.5.

October 2007 Standard 01.05. This document is up-issued to reflect changes in technical content.

- Reference to Telephony Local Area Network (TLAN) in the Introduction chapter corrected.

September 2007 Standard 01.04. This document is up-issued to reflect changes in content.

- Addition to Elements chapter as per CR Q01739494.

July 2007 Standard 01.03. This document is up-issued to reflect changes in content.

- Addition to Security management chapter as per CR Q01688518.
- Addition to Enterprise Common Manager overview chapter as per CR Q01662496.
- Addition to Enterprise Common Manager overview chapter as per CR Q01688543.

June 2007 Standard 01.02. This document is up-issued to reflect changes in content:

- Addition to Security chapter as per CR Q01639381-01.

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 reseller

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

Introduction

ATTENTION
For technical support on the Nortel version of the Linux based operating system, contact Nortel technical support through your regular channels. Do not contact Red Hat for technical support.

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 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 Telephony Local Area Network (TLAN) and Embedded Local Area Network (ELAN) network interface IP addresses for the various server types within ECM

Navigation

- "Linux installation and configuration task flow" (page 15)
- "Enterprise Common Manager overview" (page 17)
- "Security management" (page 35)
- "ECM using CLI commands configuration" (page 43)
- "Enterprise Common Manager navigation" (page 47)

Linux installation and configuration task flow

This chapter provides a high-level task flow for the installation and configuration of Subscriber Manager. You must follow the proper sequence of events to correctly install or upgrade the Linux platform base and applications. Use the task flow information in the Figure 1 "Subscriber Manager installation and configuration task flow" (page 16) to determine the proper steps for the installation or upgrade of the Linux platform base and applications.

For the complete series of task flows, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Task flow document references

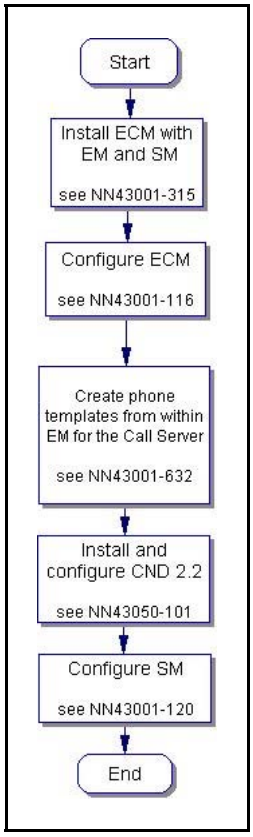
For more information, see the following documents as referenced in the task flow:

- *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*
- *Enterprise Common Manager Fundamentals (NN43001-116)*
- *Element Manager System Reference—Administration (NN43001-632)*
- *Common Network Directory 2.2 Administration (NN43050-101)*
- *Subscriber Manager Fundamentals (NN43001-120)*

The following abbreviations are used in the diagram:

- SM: Subscriber Manager
- ECM: Enterprise Common Manager
- EM: Element Manager
- CND: Common Network Directory

Figure 1
Subscriber Manager installation and configuration task flow



Enterprise Common Manager overview

Navigation

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 (or later) :

- Network Routing Service Manager for the management of Network Routing Service data, including SIP proxy and H.323 gateway
- The Communication Server 1000 (CS 1000) Element Manager for the management of CS 1000 and Meridian 1 Release 5.0 (or later)..

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

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

The following table lists the maximum number of ECMs. elements, and administrators supported for ECM client management systems.

Table 2
ECM client capacity

ECM, element, and administrator thresholds	Maximum capacity
The maximum number of elements supported in one ECM	500
The maximum total number of elements supported in multiple ECMs	500

ECM, element, and administrator thresholds	Maximum capacity
The maximum number of ECMs supported within a network	6
The maximum number of concurrent active administrators supported within an ECM network	25
The maximum number of administrators configured on one ECM	500
The maximum number of administrators connected simultaneously on one ECM	10 **ATTENTION** Although 10 administrators can be connected simultaneously, not all users can access the same elements within a system at the same time.
The maximum number of administrators connected simultaneously on the same element in a system with one or more ECMs	5

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 navigation tree.

Subscriber Manager

Subscriber Manager is deployed as a plug-in application above the ECM framework. Subscriber Manager provides a centralized location for the management of subscriber information for enterprise services. With Subscriber Manager, users can easily manage subscribers and subscriber accounts (phone services) within a network.

Prior to the ECM Subscriber Manager, subscribers and accounts were managed by individual element managers or element management systems. Subscriber Manager eliminates the need to configure and manage separate subscriber management applications for specific products in a management system.

When Subscriber Manager is installed in the ECM framework, the Subscriber link is provided in the left pane of the ECM navigation tree. From the Subscriber link, users can access the various functions to configure the required subscriber and account services for subscribers within a network.

You can also launch Subscriber Manager by navigating to the **Network, Services** Web page.

The following subscriber management functions can be performed using Subscriber Manager:

- Create subscribers
- Search subscribers
- View and update subscribers
- Delete subscribers
- Create a subscriber account
- View and update subscriber account
- Delete an account
- Publish account properties
- Synchronize accounts

Subscriber Manager allows users to add and configure phone services for subscribers with available templates in Element Manager. When configuring subscriber account phone services, the user is redirected from Subscriber Manager to Element Manager.

The following functions can be performed for subscriber phone services using Subscriber Manager:

- View and update a phone account
- Add a phone

For more information about Subscriber Manager and how to configure subscribers and subscriber accounts (phone services), see *Subscriber Manager Fundamentals (NN43001-120)*.

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

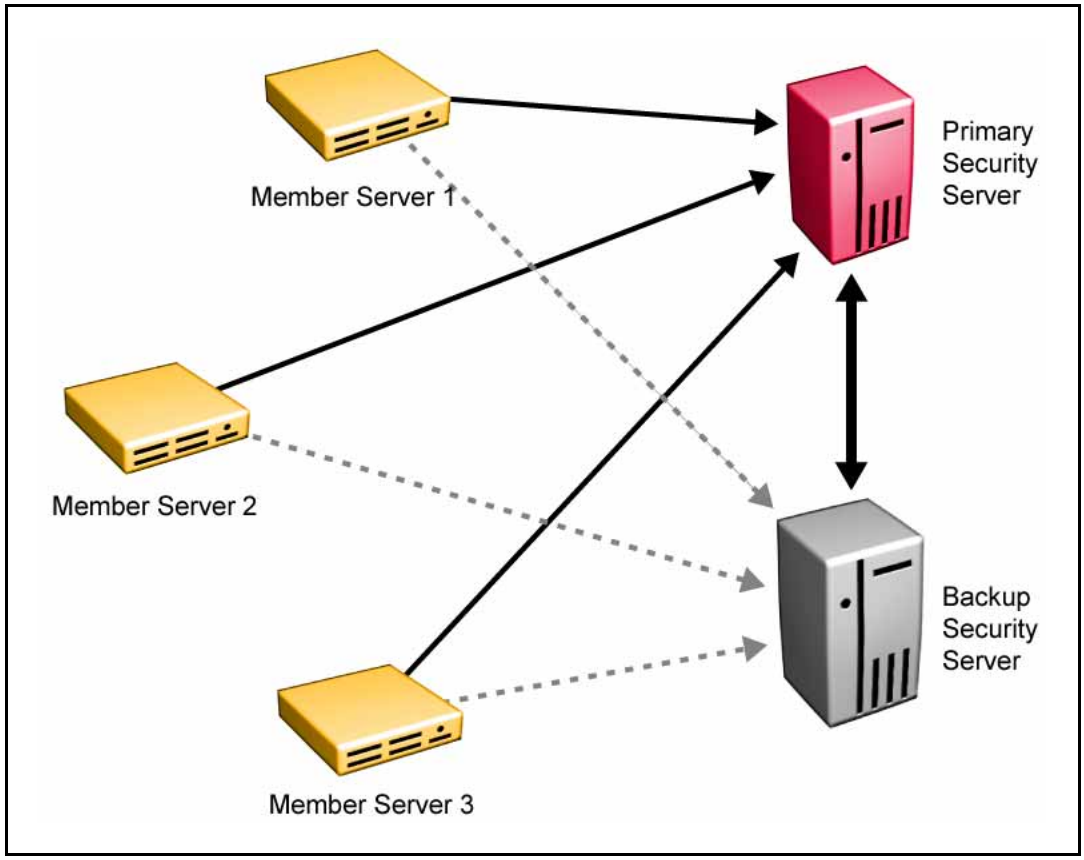
- centralized security policy administration and enforcement
- private certificate authority and X.509 certificate management
- Single Sign-On (SSO) and external Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-in User Service (RADIUS) authentication
- role- and instance-based 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 comprises 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 2 "Security domain" (page 22).

Figure 2
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 navigation tree 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. Reauthentication to access a different element within ECM is not necessary.

If a firewall exists between member servers, the backup security server, and the primary security server, the user must open the following ports.

- TCP port 5061 for SIP TLS communication
- UDP port 500 for IPsec Internet Key Exchange (IKE)
- Protocol 50 for IPsec Encapsulated Payload Protocol (ESP)
- 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 636 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 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 item.

  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 an element from the Favorites list in the browser window.

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

  To add an element to your Favorites list, 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 items, 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 items appear in the left navigation pane.

Click the Common Manager item 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 5.5, the following built-in certificates types are supported:

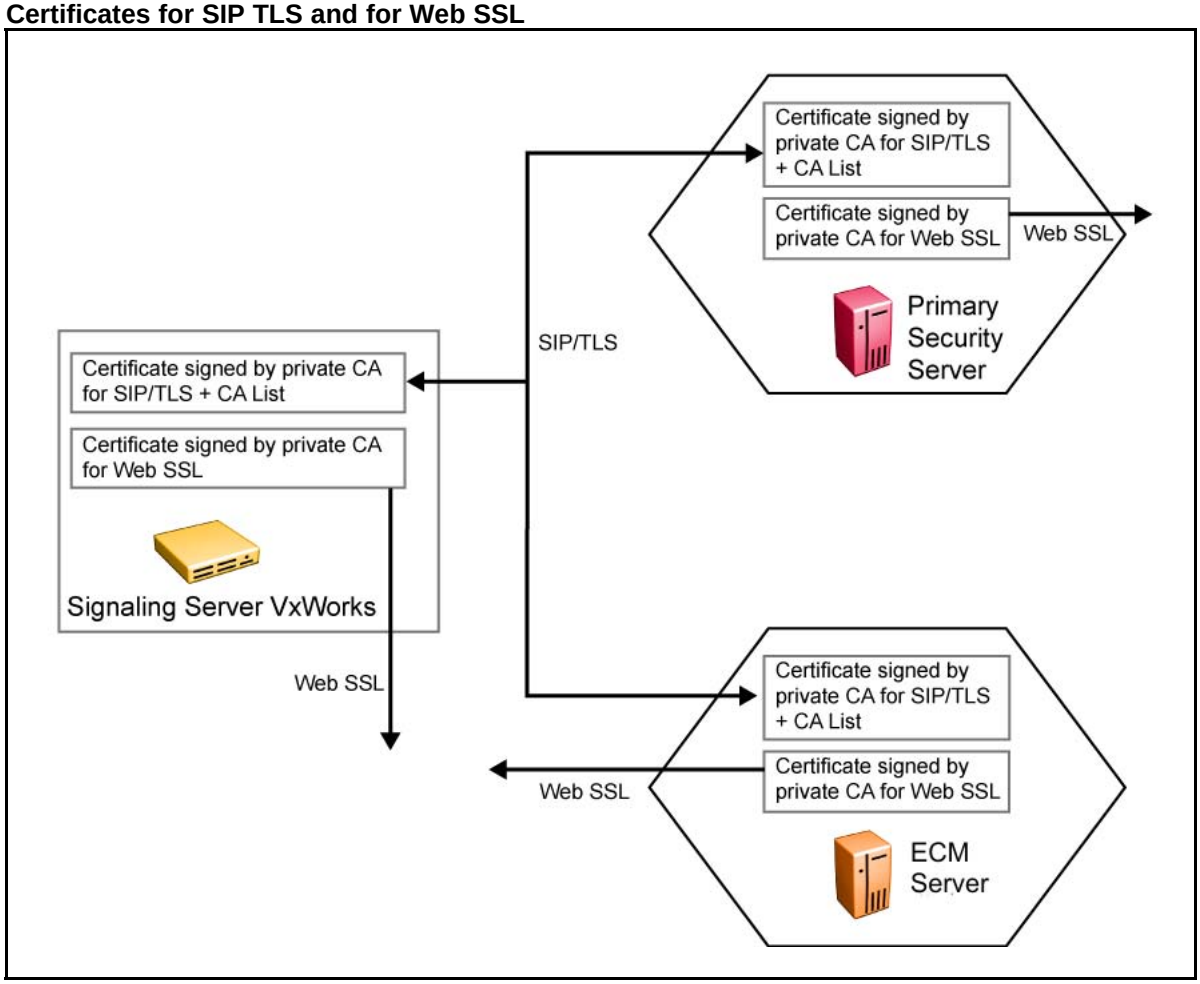
- Web interface using Secure Sockets Layer (Web SSL)
- Session Initiation Protocol signaling using Transport Layer Security (SIP TLS)

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 3 "Certificates for SIP TLS and for Web SSL" (page 25).

Figure 3
Certificates for SIP TLS and for Web SSL



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, and 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.

It is best practice to configure both a primary and a backup security server per ECM security domain to assure a highly available authentication and authorization service for OA and M users who need to access managed systems/elements in the ECM security domain, as well as for auxiliary applications that rely on continuous availability of the ECM framework Web services API to monitor and control the CS 1000.

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 media provide eight 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) DVD provides the following five 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)
- The Primary ECM Server (install EM, Subscriber Manager, and the primary ECM security service)
- A Backup ECM Server (install EM, Subscriber Manager, and a backup ECM security service)

ATTENTION
The first Linux server must be installed with the primary security service. Install the second Linux server with the backup security service, and then install any other required Linux servers. 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. For more information about adding elements, see "Add elements" (page 58).

ATTENTION
Nortel recommends that you install Element Manager on ECM as the primary security server before you install Linux-based NRS, and that you configure all the NRS in a single ECM security domain.

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

After the Linux base is installed and before the CS 1000 applications are installed, host configuration scripts have to be run on every server in the ECM security domain. For more information on running the host configuration scripts see "Host configuration" (page 43).

Domain Name System

During the Linux base installation, users are prompted to configure the Domain Name System (DNS) server IP address. Users can also manually configure the DNS after the Linux base is installed. The DNS server IP address is stored in /etc/resolv.conf.

For more information about configuring the DNS server, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*

By default, Linux uses the DNS lookup to find the Fully Qualified Domain Name (FQDN) to IP or IP to FQDN address mapping as configured in /etc/nsswitch.conf. If a DNS server in the /etc/resolve.conf is configured but unreachable, each DNS lookup/reverse lookup can take up to five seconds to time-out.

The central logging utility in ECM relies on an IP address to FQDN reverse lookup to map Web client IP addresses to FQDN. When the DNS server in /etc/resolv.conf is unreachable, accessing Web resources in ECM can take longer due to the five second time-out in the reverse DNS lookup.

Users can perform the following three tasks to resolve the DNS server unreachable time-out issue:

- Remove the unreachable DNS server IP address from /etc/resolv.conf or change it to a DNS server IP address that is reachable by the Linux server.
- Remove the DNS option from the hosts entry in /etc/nsswitch.conf to stop the DNS lookup.
- Use the Linux base CLI command hostconfig to add the Web client IP address to FQDN mapping in the Linux server to /etc/hosts.

  Since the IP address to FQDN mapping and the FQDN to IP address mapping is always queried from the /etc/hosts first, the DNS will not be triggered if the mapping can be found in the /etc/hosts.

ATTENTION

To check the reverse lookup, 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, and run the **`nslookup <IP address of the DNS>`** command line interface (CLI) script.

If the reverse lookup to the DNS server failed, you must configure the DNS server.

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 3 "Types of log files in ECM" (page 29) describes the types of log files based on their content.

Table 3
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 4 "Audit security logs available in the ECM security framework" (page 30) describes the two types of audit security logs stored in the ECM security framework.

Table 4
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.

Table 5 "ECM log files" (page 30) describes the log files supported in ECM. Log files are stored on the primary security server in /opt/nortel/logs/3rd_party/security/s1is/logs.

Table 5
ECM log files

Log file	Description
amauthentication.nlog	Record user login and logout activities.
amconsole.nlog	Record user actions performed through the AM server administration console such as creation, deletion, and modification of identity-related objects, realms, and policies.
amfederation.nlog	Associated with Sun Access Manager federation service.
ampolicy.nlog	Record policy-related events such as policy creation, deletion, modification, and evaluation.
amsso.nlog	Record session management attributes values such as login time, logout time, and timeout limits.
application.alog	Record events from internal applications such as NSS switch module, etc.
bcc.alog	Record events from BCC module.
bccWebService.alog	Record events from BCC Web service.
certificateManagement.nlog	Record certificate related events such as creation, deletion, and modification of end point certificates and trusted Certificate Authority list.
cs1000-em.alog	Record CS 1000 EM specific events.
cs1000WebService.alog	Record events from CS 1000 Web service.

Log file	Description
managedElementRegistryService.alog	Record events from managed element registry Web service.
mftauthentication.alog	Record events from Nortel plug-in authentication modules.
nrsm.alog	Record events from NRSM module.
nrsmWebService.alog	Record events from NRSM Web service.
quantum.alog	Record ECM specific events.
security.nlog	Record security administration activities such as create, modify, or delete users, roles, or elements.
subscriberManager.alog	Record events from Subscriber Manager.
sunoneis.nlog	Record all other logs to this file.

If the DNS server is configured but is offline, there will be a delay in accessing the ECM Web interface. To avoid this, the PC client's FQDN should be added into the /etc/hosts file of the ECM server.

High Availability configuration

High Availability (HA) provides continuous availability and reliability in case of failure or abnormal termination of the active server. During the installation of the backup security server, the high availability is automatically configured between the primary security server and backup security server.

Table 6 "Failover scenarios for the primary and backup security servers" (page 32) shows the ECM HA failover scenarios for the primary and backup security servers.

Table 6
Failover scenarios for the primary and backup security servers

Primary security server	Backup security server	Failover scenario
offline	online	• The ECM servers inside the same security domain that use the primary security server will failover automatically to the backup security server in approximately five minutes. **ATTENTION** Users must use the Linux base CLI command hostconfig (used for configuring the IP to FQDN mapping) to add the backup security server if the DNS is not configured. • The ECM server inside the primary security server will failover automatically to the backup security server in approximately five minutes. Configure the backup server FQDN from the member server.
online	offline	• The ECM servers inside the same security domain that use the backup security server will failover automatically to the primary security server in approximately five minutes. • The ECM server inside the backup security server will failover automatically to the primary security server in approximately five minutes.

When the ECM servers failover from the primary security server to the backup security, the DNS must be configured to retrieve the IP from the FQDN of the backup security server. Use the Linux base CLI command dnsconfig to configure the DNS settings on each server.

ATTENTION
If the backup security server is reinstalled, users must run a CLI command script to clear the HA between the primary security server and the backup security server, see “Linux root account command line interface commands” (page 149).

If any changes are required for the external authentication servers or authentication scheme after the backup security is installed, users must run a CLI command script on the primary security server and the backup security server to restart the Sun Access Manager Web server, see “Linux root account command line interface commands” (page 149).

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 141).

Security management

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.

ATTENTION
The pages are view only, unless you have been given permissions to perform operations like editing and deleting.

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

Navigation

- "Authentication" (page 35)
- "Security policies" (page 37)
- "Access control policies" (page 39)

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.

The following table lists the status types for a local user account.

Table 7
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.

The following table describes the supported built-in account for ECM.

Table 8
Supported built-in account

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

ATTENTION
With the built-in administrator 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 Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-in User Service (RADIUS), the external administrator account is added to ECM.

For Release 5.0 (or later), 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.

ATTENTION
The security administrator role is not available for external LDAP users.

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 9 "Password aging policy thresholds" (page 38) describes what occurs when a user logs into ECM when the password aging policy thresholds expire.

Table 9
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.

The default password strength policy enforcement

The default password strength policy requires a password to contain a minimum of eight alphanumeric characters. In addition to letters and numeric digits, the password must contain one special character, such as an exclamation mark (!). The password must contain a combination of alphanumeric and special 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 one of the N previously used passwords, the password is rejected. N is defined by the ECM administrator. The default value of N is 6.

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. By default the user is locked out after 3 failed attempts.

Users can change the password policies from the Password Policy Web page, as shown in “Editing password policies” (page 123).

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 “Editing the login warning banner” (page 128).

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 “Editing the authentication scheme” (page 120).

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 10 "Features supported in the ECM security access control service" (page 40) 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 10
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, “Example of a least privilege algorithm” (page 153) 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 11 "Built-in roles" (page 41) describes the built-in role permission assignment for the ECM security framework.

Table 11
Built-in roles

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

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 12 "Built-in role permission assignments for CS 1000 elements" (page 42) shows the built-in role permission assignments for CS 1000 elements.

Table 12
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
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
PowerUser	Give the user all of the permissions for CS 1000.

Table 13 "Built-in role permission assignments for the Network Routing Service" (page 42) shows the built-in role permission assignments for the Network Routing Service.

Table 13
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
NrsmMonitor	The user has read-only access to Network Routing Service elements.
PowerUser	The user can perform operations, administration, and maintenance on the Network Routing Service.

For an example of role- and instance-based access control, role permission assignments, and user role assignments for users in ECM, see “Example of role- and instance-based access control in CS 1000 systems” (page 155).

ECM using CLI commands configuration

This chapter contains information on configuring ECM using command line interface (CLI) commands. For each CLI command, log on to the CLI with a root account and run the CLI command script.

Navigation

- "Host configuration" (page 43)
- "Configure system account passwords" (page 44)

Host configuration

After the Linux base is installed and before the CS 1000 applications are installed, host configuration scripts have to be run on every server in the ECM security domain. Use the steps in "Configuring hosts" (page 43) to configure the hosts. For more information on installing Linux and the CS 1000 applications, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)* () .

Configuring hosts

Step	Action
1	Log on to the primary security server CLI using SSH or port console.
2	At the prompt, enter **su** to switch to superuser mode.
3	At the prompt, enter the root password.
4	Run the **/home/nortel/bin/hostconfig add -ip <SECONDARY SERVER IP> -host <SECONDARY SERVER HOST NAME> -domain <SECONDARY SERVER DOMAIN NAME>** script.
5	Log on to the secondary security server CLI using SSH or port console.
6	At the prompt, enter **su** to switch to superuser mode.

7 At the prompt, enter the root password.

8 Run the **/home/nortel/bin/hostconfig add -ip <PRIMARY SERVER IP> -host <PRIMARY SERVER HOST NAME> -domain <PRIMARY SERVER DOMAIN NAME>** script.

9 Log on to each member security server CLI using SSH or port console.

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

11 At the prompt, enter the root password.

12 Run the **/home/nortel/bin/hostconfig add -ip <PRIMARY SERVER IP> -host <PRIMARY SERVER HOST NAME> -domain <PRIMARY SERVER DOMAIN NAME>** script.

13 Run the **/home/nortel/bin/hostconfig add -ip <SECONDARY SERVER IP> -host <SECONDARY SERVER HOST NAME> -domain <SECONDARY SERVER DOMAIN NAME>** script.

--End--

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 the Identity Server client (isclient) application on all servers in the security domain.

The isclient application is installed on the Primary, Backup, and Member servers. This application provides the following services: SSH trust management, HA configuration, backup and restore functionality, log rotate and change password for the default security services account password.

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 following procedure 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.

Changing the system account password from the primary security service

Step	Action
1	Log on to the primary security server CLI using SSH or port console.
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. ***Note:*** If the password change operation fails during application installation or during the execution of the above script, execute the command **`/opt/nortel/sunAm/shell/security_service_startup.sh`** as a root user and then change the password with the above 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 following procedure to send the system account password changes to the isclient on the primary security server, the backup security server, member server and if the servers are offline when the system account password is changed from the primary security service.

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 CLI using SSH or port console.
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. A new password is not required. 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 "Resetting a user password from the CLI" (page 46) to reset the password from the CLI.

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 ECM administrative user name to change.
6	Enter a new password.
7	Confirm the new password.

--End--

Enterprise Common Manager navigation

This chapter provides a description of the items 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.

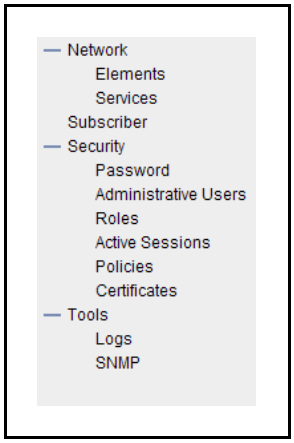
Navigation

- Enterprise Common Manager navigation tree
- “Logging into ECM for the first time” (page 50)
- “Log on options in ECM” (page 52)
  - “Log on with Web authorization servlet from the backup security server” (page 52)
  - “Log on with Single Sign-On for Web-based applications using the Fully Qualified Domain Name” (page 53)
  - “Log on with SSO between Web applications in multiple ECMs” (page 54)
- “Log off options” (page 55)

Enterprise Common Manager navigation tree

The ECM framework navigation tree is located on the left side in the navigation pane as shown for the primary security server in the following figure.

Figure 4
ECM navigation tree



When Subscriber Manager is installed in ECM, the ECM navigation tree has a Subscriber link as shown for the primary security server in Figure 4 "ECM navigation tree" (page 48).

Items in the navigation pane are structured as follows:

- **Network**
  - Elements
  - Services
- **Subscriber**
- **Security**
  - Password
  - Administrative Users
  - Roles
  - Active Sessions
  - Policies
  - Certificates
- **Tools**
  - Logs
  - SNMP

Network

The ECM Network is defined by the Elements and Services within the scope of its security framework.

- 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.
- Services: The Services section contains links to the managed services. From this Web page, users can edit basic details of installed services. For Release 5.5, the only supported service is Subscriber Manager.

Subscriber

This is a short cut link to the Subscriber Manager application user interface. Alternatively the user can access this interface indirectly via the **Services** link. For more information about Subscriber Manager, see *Subscriber Manager Fundamentals (NN43001-120)*.

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.
- Administrative 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.
- Active 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.

Logging into ECM for the first time

Use the steps in "Changing the ECM default password" (page 50) 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.

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 the following figure.

Figure 5
Login Web page

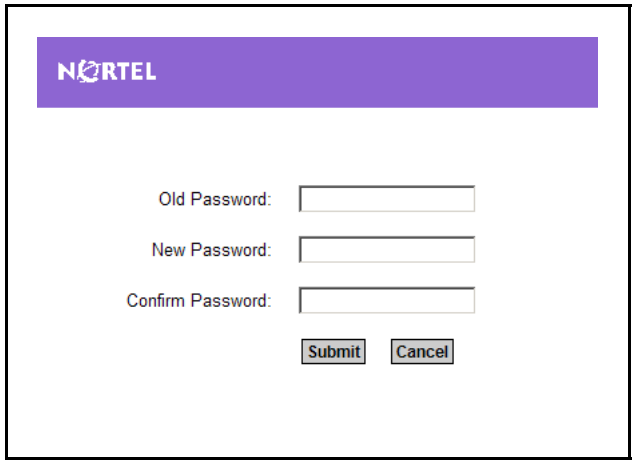
3 In the **User ID** field, type **admin**.

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 with a prompt to change the password, as shown in the following figure.

Figure 6
Nortel Web page

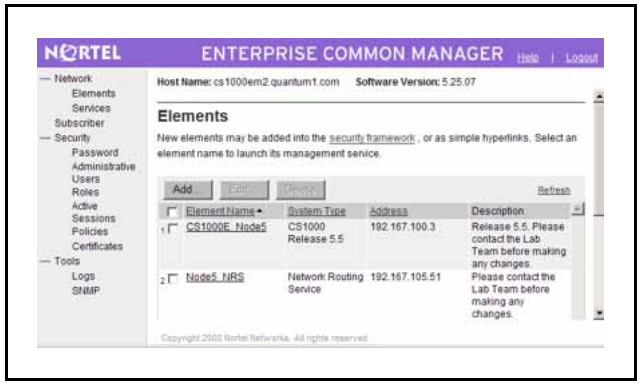


5 From the Nortel Web page, perform the following tasks:

- 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 the following figure.

Figure 7
Enterprise Common Manager navigation Web page



--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 with Web authorization servlet from the backup security server

Use the following procedures to log on to the backup security service with the webauth servlet.

Logging on to the backup security server with webauth servlet

Step	Action
1	In a Web browser, type **`https://<fqdnOfBackupSecurityServer>:58081/webauth/webauthservlet`** to log on to ECM. The login page appears.
2	Enter a valid user name and password combination, and click **Login**. The backup security server authentication Web page opens, as shown in the following figure.

Figure 8
Backup security server authentication Web page

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

The ECM backup security server navigation Web page appears.

Note: The Subscriber, Administrative Users, Policies, Certificates and Logs links are 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 following procedures 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.

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 following procedures 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.

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

The following table 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 14
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 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

This chapter contains information on managing elements in ECM.

Navigation

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 Network branch of the ECM navigation tree, 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 5.0 (or later)
- Network Routing Service
- SIP Gateway

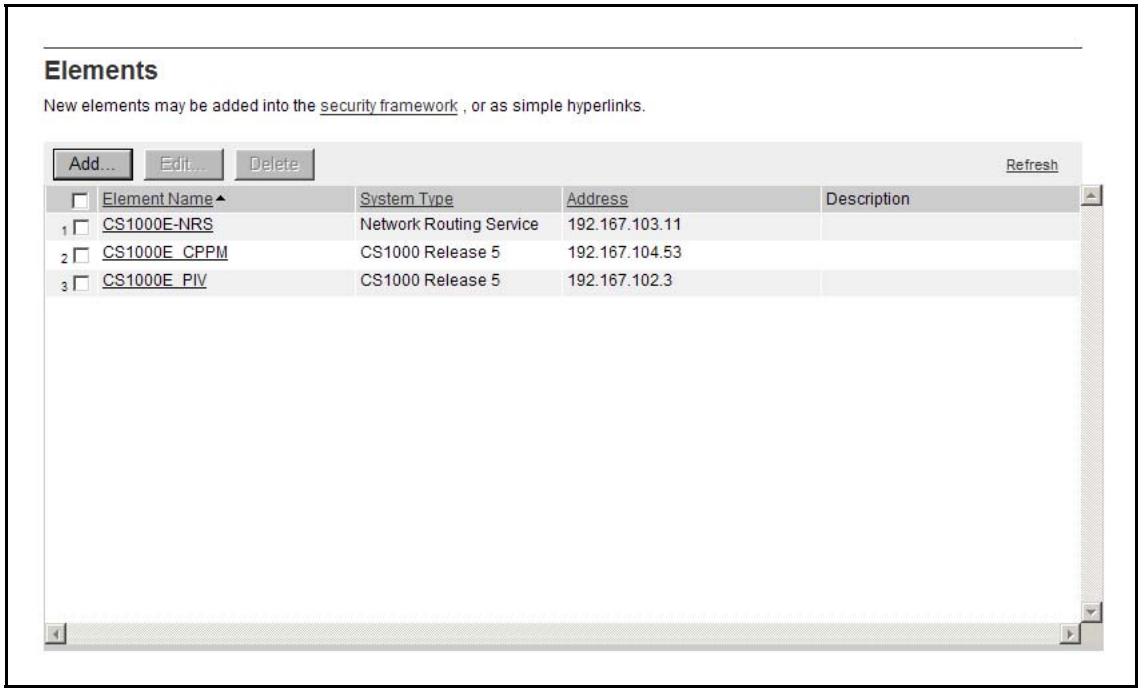
Launch a managed element

Use the following procedure 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.

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 the following figure.

Figure 9
Elements Web page



3	In the **Element Name** column, click an item. 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 item and select **Add to favorites**.

--End--

Add elements

To add an element to ECM, the element must be named and its management address (URL) defined, so that ECM users can navigate to it. Then the element must be incorporated into the security framework

by mapping authorization permissions offered by the element to user roles created in ECM. This role-permission mapping allows group-based authorization across all elements under the security umbrella of ECM. Individual user capabilities are limited by the role(s) to which they are assigned.

The role-permission mapping can be added to an element with the **Edit Mapping** or **Copy All From** functionality of ECM.

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

Nortel recommends that you use a consistent naming convention when you add the systems and devices as elements in ECM to make management easier.

The following table shows an example of a good naming convention for elements installed in ECM.

Table 15
Element naming conventions

Element	Recommended naming convention
CS 1000 system	<system name>
CS 1000 Signaling Server	<system name> Node ID <IP Telephony Node ID number>_Leader | Follower_1 |

Note: The Refresh link on the Elements page should be clicked if the user is not able to add new elements or delete selected elements after the security service is restarted.

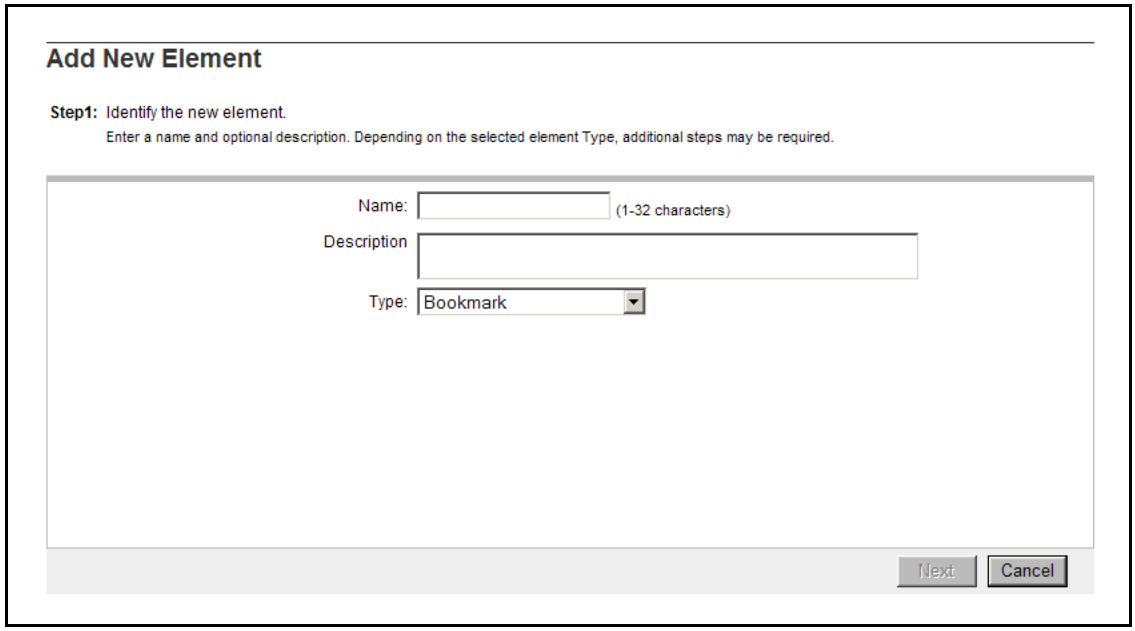
Add a bookmark

Use the following procedures to add an external hyperlink element in ECM.

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 opens, as shown in Figure 9 "Elements Web page" (page 58).
3	From the **Elements** Web page, click **Add**. The Add New Element Step 1 page opens, as shown in the following figure.

Figure 10
Add New Element Step 1 Web page



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

ATTENTION
The name must be from 1 to 32 characters.

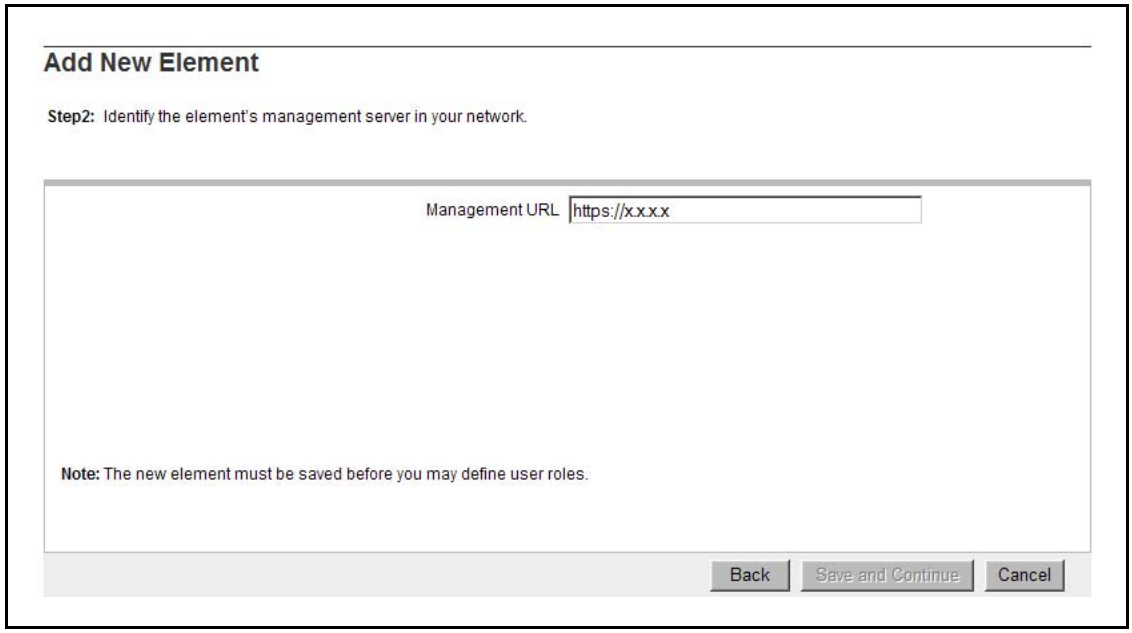
5 In the optional **Description** field, type a description if required.

6 From the **Type** list, select **Bookmark**.

7 Click **Next**.

The Add New Element Step 2 Web page opens for the Bookmark element, as shown in the following figure.

Figure 11
Add New Element Step 2 Web page

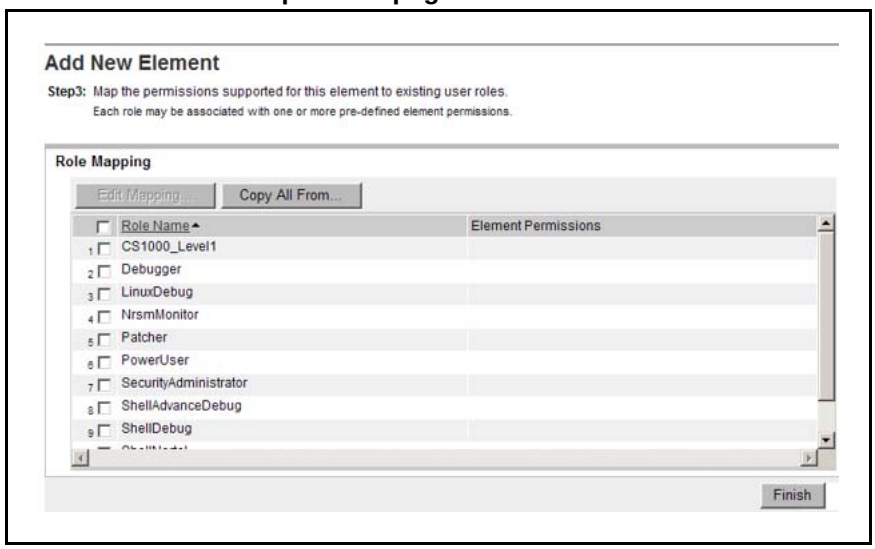


8 In the **Management URL** field, type the URL for the Bookmark element.

9 Click **Save and Continue**.

The Add New Element Step 3 Web page opens, as shown in the following figure.

Figure 12
Add New Element Step 3 Web page

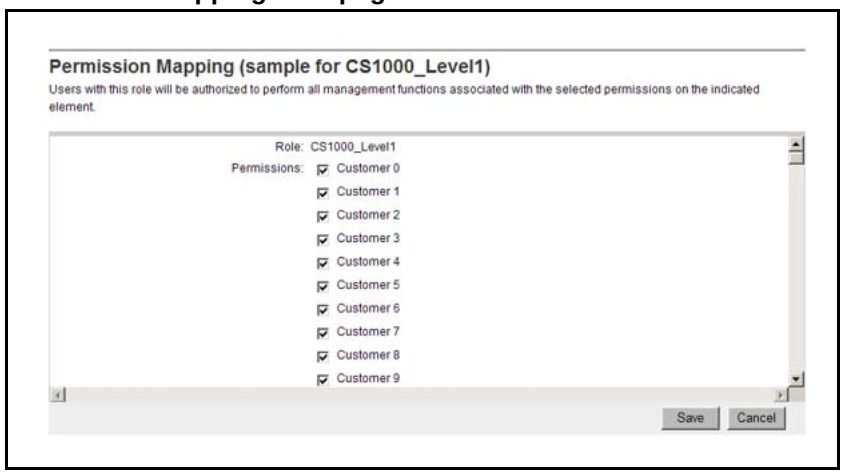


10 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.

The Permission Mapping Web page opens for the selected role, as shown in the following figure.

Figure 13
Permission Mapping Web page



2. Select or clear the permissions for the element and click **Save**.
   The Add New Element Step 3 Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The Elements Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The Copy element Web page appears, as shown in the following figure.

Figure 14
Copy element Web page

Note: If there are no elements of this type from which to copy, the Add New Element Step 3 Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The Add New Element Step 3 Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The Elements Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

Add a CS 1000 element

Use the following procedure to add a CS 1000 element in ECM.

Procedure 1
Adding a CS 1000 element

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The Elements Web page opens, as shown in Figure 9 "Elements Web page" (page 58).
3	From the **Elements** Web page, click **Add**. The **Add New Element Step 1** page opens, as shown in Figure 10 "Add New Element Step 1 Web page" (page 60).
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.

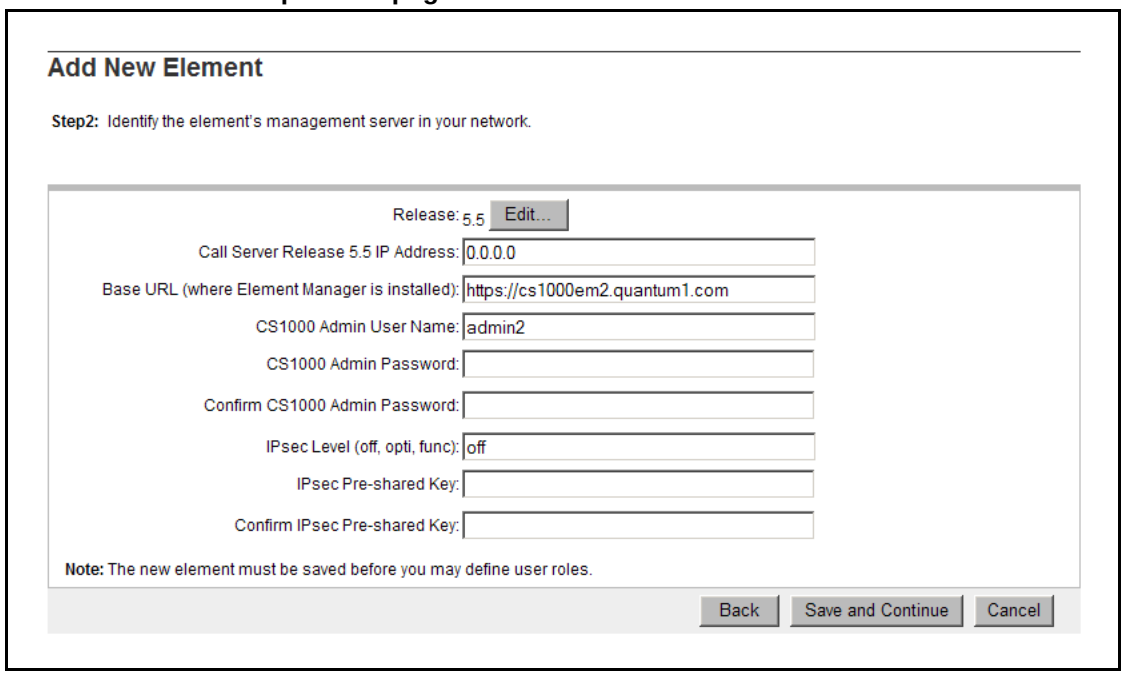
5 In the optional **Description** field, type a description if desired.

6 From the **Type** drop down list, select **CS1000**.

7 Click **Next**.

The **Add New Element Step 2** Web page opens, as shown in Figure 15 "Add New Element Step 2 Web page" (page 64).

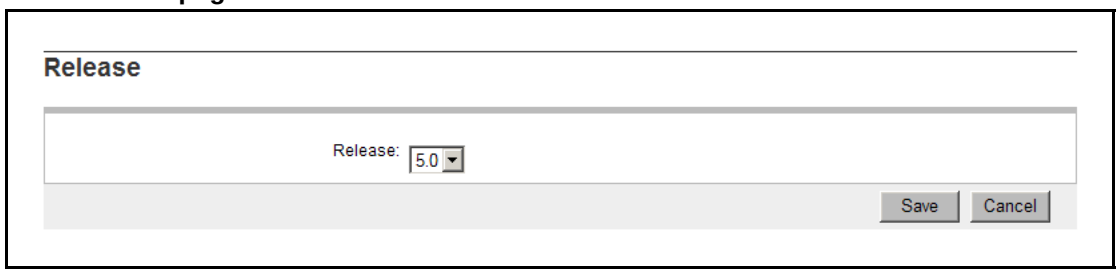
Figure 15
Add New Element Step 2 Web page



8 Review the **Release** type.

If the Release is incorrect, click **Edit** beside the **Release** box and select the desired Release from the available list, as shown in Figure 16 "Release Web page" (page 64).

Figure 16
Release Web page



9 Click **Save** to save your change or **Cancel** to cancel the change.

You are returned to the **Add New Element Step 2** Web page.

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

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

The default value is where Element Manager is installed.

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 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, retype the password.

15 Type the **IPsec** level in the **IPsec Level** text box.

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. Failure 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 16 "Mismatched IPsec levels on CS 1000 and ECM" (page 66).

Table 16
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, retype the IPsec preshared key.

18 Click **Save and Continue**.

The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61).

19 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.

The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--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 “Edit the properties for a CS 1000 element” (page 74). 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>

Add a Network Routing Service element

Use the steps in “Adding a Network Routing Service element” (page 68) to add a Network Routing Service element in ECM.

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 opens, as shown in Figure 9 "Elements Web page" (page 58).
3	From the **Elements** Web page, click **Add**.

The **Add New Element Step 1** page opens, as shown in Figure 10 "Add New Element Step 1 Web page" (page 60).

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.

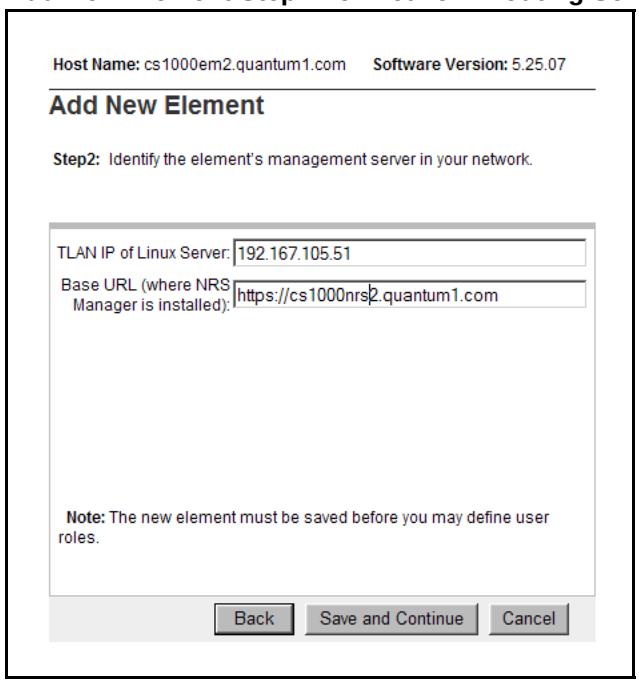
5 In the optional **Description** field, type a description if desired.

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

7 Click **Next**.

The **Add New Element Step 2 for Network Routing Service** Web page opens, as shown in Figure 17 "Add New Element Step 2 for Network Routing Service" (page 69).

Figure 17
Add New Element Step 2 for Network Routing Service



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.

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 Click **Save and Continue**.

The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61).

11 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

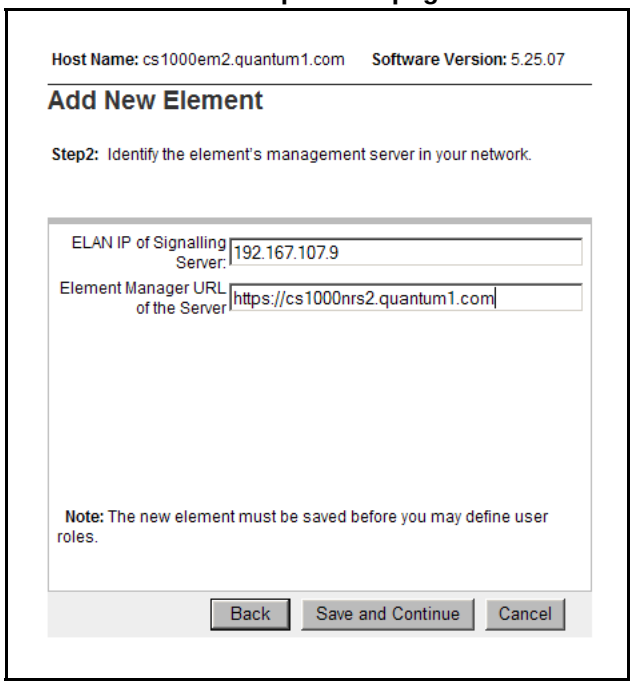
Add a SIP Gateway element

Use the steps in “Adding a SIP Gateway element” (page 71) to add a VxWorks-based signaling server element in ECM.

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 opens, as shown in Figure 9 "Elements Web page" (page 58).
3	From the **Elements** Web page, click **Add**. The **Add New Element Step 1** page opens, as shown in Figure 10 "Add New Element Step 1 Web page" (page 60).
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** drop down list, select **SIP Gateway**. The **Add New Element Step 2** Web page for SIP Gateway appears, as shown in Figure 18 "Add New Element Step 2 Web page for SIP Gateway" (page 71)

Figure 18
Add New Element Step 2 Web page for SIP Gateway



7	Click **Next**.

8 In the **ELAN IP of Signalling Server** field, type the ELAN 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**.

The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61).

11 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Add New Element Step 3** Web page opens, as shown in Figure 12 "Add New Element Step 3 Web page" (page 61). Users can select a different role to map permissions to the element.
3. Click **Finish**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

Edit element properties

Use the procedures in this section to edit the properties and role-permission mapping of a Bookmark, CS 1000 Release 5.0 (or later) , Network Routing Service, or SIP Gateway element installed in ECM.

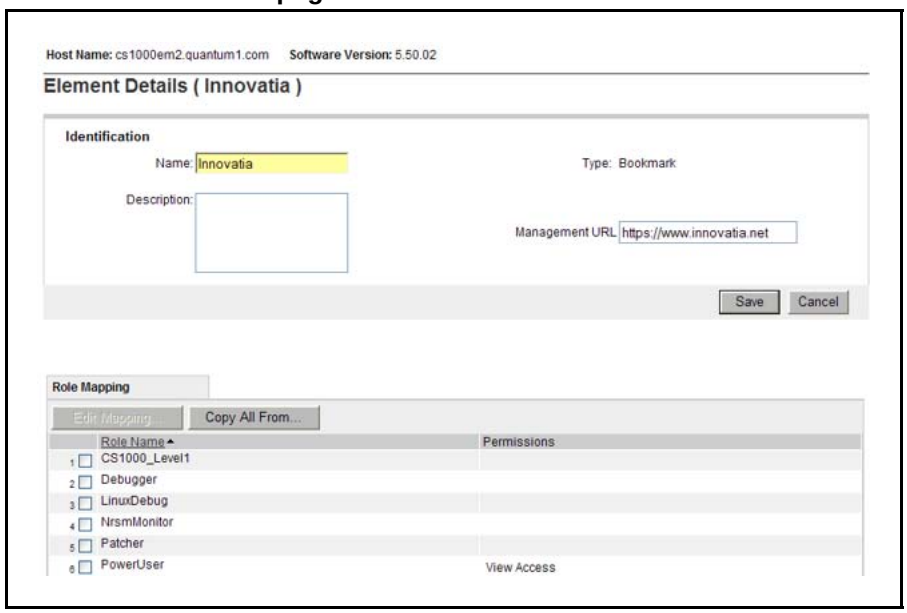
Edit the properties of a bookmark element

Use the following procedure to edit the properties of a bookmark element in ECM.

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 9 "Elements Web page" (page 58).
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 the following figure.

Figure 19
Element Details Web page for a bookmark element



5	From the **Identification** section, edit the following fields as required: • Name • Description • Management URL

6 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The Permission Mapping Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The Element Details Web page for the selected bookmark element appears, as shown in Figure 19 "Element Details Web page for a bookmark element" (page 73). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The Elements Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The Copy element Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the Add New Element Step 3 Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The Element Details Web page for the selected bookmark element appears, as shown in Figure 19 "Element Details Web page for a bookmark element" (page 73). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The Elements Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

Edit the properties for a CS 1000 element

Use the steps in "Editing the properties of a CS 1000 element" (page 74) to edit the properties of a CS 1000 element.

Editing the properties of a CS 1000 element

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

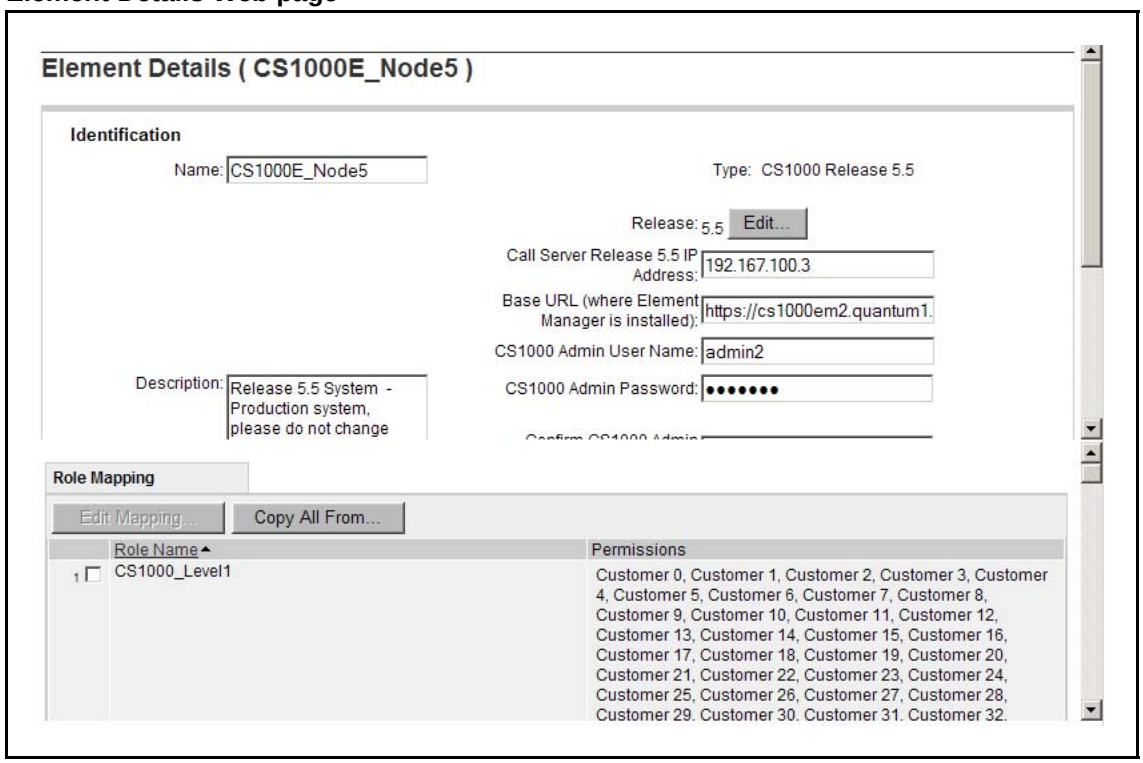
2 From the navigation pane, click **Elements**.

The **Elements** Web page appears, as shown in Figure 9 "Elements Web page" (page 58).

3 From the **Elements** Web page, select the check box beside the CS 1000 element to edit, and click **Edit**.

4 The **Element Details** Web page appears, as shown in Figure 20 "Element Details Web page" (page 75).

Figure 20
Element Details Web page



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

- Release
  If the Release is incorrect, click **Edit**.
  The CS 1000 Release Web page appears.
  From the **Release** list, select the desired Release from the available list. Click **Save** to save the changes or click **Cancel** to cancel the changes.
- Name
- Description
- Call Server IP Address
- Base URL (where Element Manager is installed)
- 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 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Element Details** Web page for the selected CS 1000 element appears, as shown in Figure 20 "Element Details Web page" (page 75). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Element Details** Web page for the selected CS 1000 element appears, as shown in Figure 20 "Element Details Web page" (page 75). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

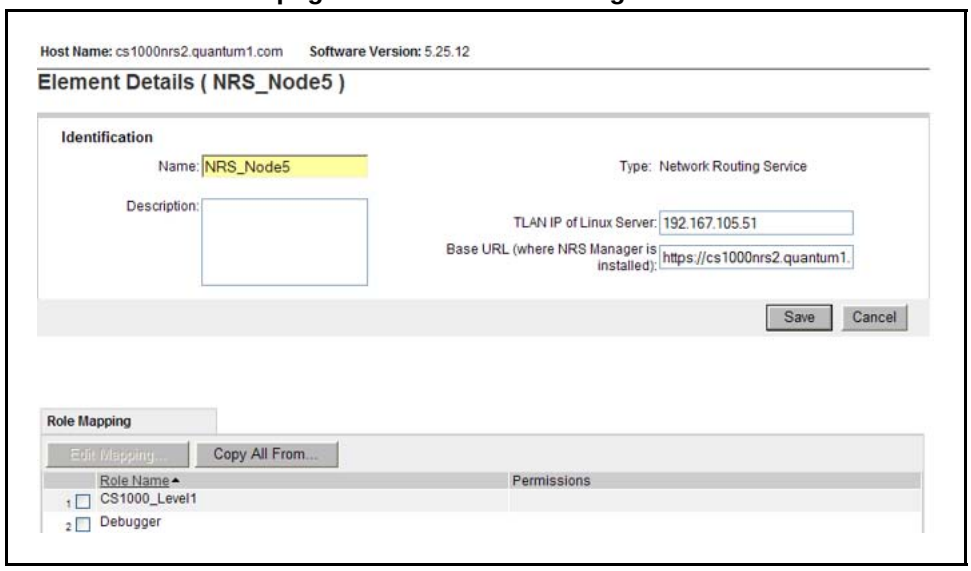
Edit the properties for a Network Routing Service element

Use the steps in “Editing the properties of a Network Routing Service element” (page 77) to edit the properties of a Network Routing Service element.

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 9 "Elements Web page" (page 58).
3	From the **Elements** Web page, select the check box beside the Network Routing Service element to edit, and click **Edit**.
4	The **Element Details** Web page appears, as shown in Figure 21 "Element Details Web page for a Network Routing Service element" (page 77).

Figure 21
Element Details Web page for a Network Routing Service element



Step	Action
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)
6	From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Element Details** Web page for the selected Network Routing Service element appears, as shown in Figure 21 "Element Details Web page for a Network Routing Service element" (page 77). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Element Details** Web page for the selected Network Routing Service element appears, as shown in Figure 21 "Element Details Web page for a Network Routing Service element" (page 77). Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

Edit the properties for a SIP Gateway element

Use the following procedure to edit the properties of a SIP Gateway element.

Editing the properties of a SIP Gateway element

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

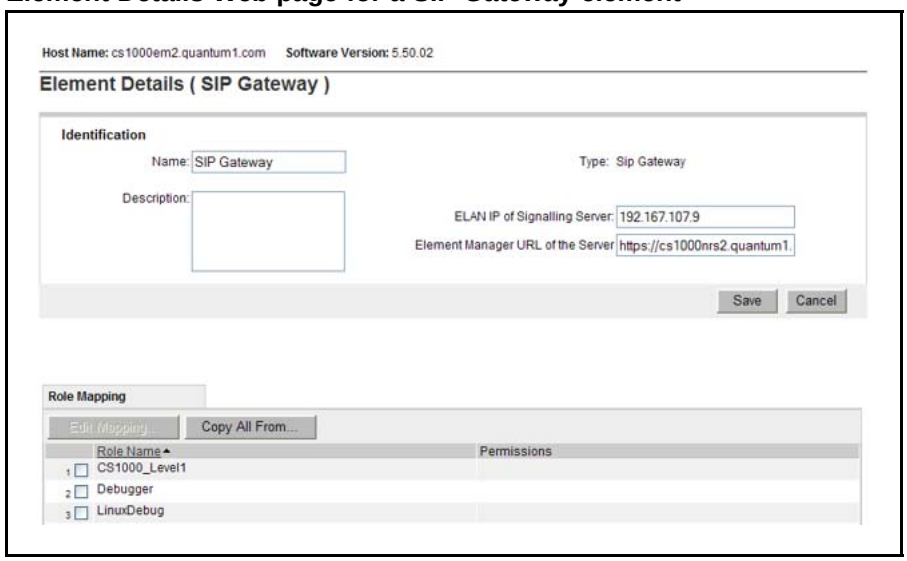
2 From the navigation pane, click **Elements**.

The Elements Web page appears, as shown in Figure 9 "Elements Web page" (page 58).

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

4 The Element Details Web page appears, as shown in the following figure.

Figure 22
Element Details Web page for a SIP Gateway element



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

- Name
- Description
- ELAN IP of Signaling Server
- Element Manager URL of the Server

6 From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role.

1. Click **Edit Mapping**.
   The **Permission Mapping** Web page opens for the selected role, as shown in Figure 13 "Permission Mapping Web page" (page 62).
2. Select or clear the permissions for the element and click **Save**.
   The **Element Details** Web page for the selected SIP Gateway element appears, as shown in Figure 22 "Element Details Web page for a SIP Gateway element" (page 79).

Users can select a different role to map permissions to the element.

3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

Or

1. Click **Copy All From**.
   The **Copy element** Web page appears, as shown in Figure 14 "Copy element Web page" (page 63)

   Note: If there are no elements of this type from which to copy, the **Add New Element Step 3** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Element Details** Web page for the selected SIP Gateway element appears, as shown in Figure 22 "Element Details Web page for a SIP Gateway element" (page 79).
   Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Elements** Web page opens, as shown in Figure 9 "Elements Web page" (page 58).

--End--

Delete selected elements

Use the steps in “Deleting selected elements” (page 80) to delete elements that ECM no longer requires.

Note: The Refresh link on the Elements page should be clicked if the user is not able to add new elements or delete selected elements after the security service is restarted.

Deleting selected elements

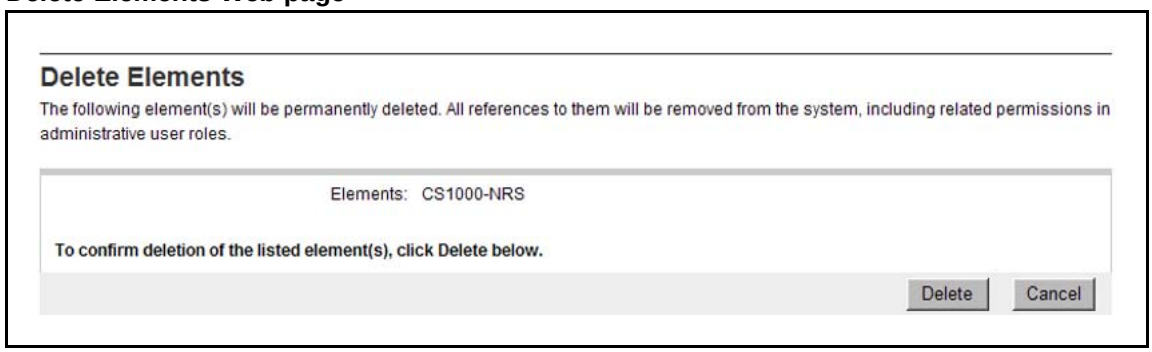
Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Elements**. The **Elements** Web page appears, as shown in Figure 9 "Elements Web page" (page 58).

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 23 "Delete Elements Web page" (page 81).

Figure 23
Delete Elements Web page



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

--End--

ATTENTION
Accessing management applications of a deleted elementECM 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.

Services

Contents

This chapter contains the following topics:

Manage services

Subscriber Manager

For Release 5.5, Subscriber Manager is deployed as a plug-in application above the ECM framework. Subscriber Manager provides a centralized location for the management of subscriber information for enterprise services. With Subscriber Manager, users can easily manage subscribers and subscriber accounts (phone services) within a network.

For more information about Subscriber Manager see Subscriber Manager and *Subscriber Manager Fundamentals (NN43001-120)*.

There are two ECM installation media: a Network Routing Service (NRS) application Install CD and an Element Manager (EM) application Install DVD. ECM Framework, EM and Subscriber Manager are installed from the EM application Install DVD. For more information on installing ECM, EM and Subscriber Manager, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

For more information about how to configure subscribers and subscriber accounts (phone services) with Subscriber Manager, see *Subscriber Manager Fundamentals (NN43001-120)*.

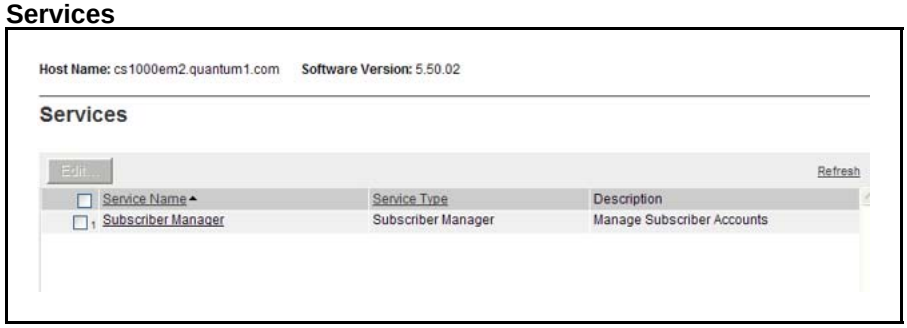
Launch a managed service

Use the steps in Procedure 2 “Launching a managed service” (page 84) to launch the management application for a selected service in the current or a new Web browser.

Procedure 2
Launching a managed service

Step	Action
1	Log on to ECM .
2	From the navigation pane, click **Network, Services**. The Services Web page opens, as shown in Figure 24 "Services" (page 84). ***Note:*** When there are no services configured, the Services Web page contains a message indicating “No Network Services are configured”.

Figure 24
Services



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

--End--

Add services

Use the steps in “Adding Subscriber Manager” (page 84) to add Subscriber Manager as a service in ECM.

Adding Subscriber Manager

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

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

The **Roles** Web page opens, as shown in Figure 35 "Roles Web page" (page 100).

3 Click **Add**.

The **Add New Role Step 1** Web page opens, as shown in Figure 36 "Add New Role Step 1" (page 101).

4 In the **Role Name** field, type a unique name, for example, Subscriber Manager.

5 In the **Role Description** field, type a description.

6 Click **Save and Continue**.

The Add New Role Step 2 Web page opens, as shown in Figure 37 "Add New Role Step 2" (page 102).

7 Click **Finish**.

The **Roles** Web page opens.

8 From the navigation pane, click **Services**.

The **Services** Web page opens, as shown in Figure 24 "Services" (page 84).

9 From the **Services** Web page, select the check box beside **Subscriber Manager** and click **Edit**.

The **Service Details** Web page for Subscriber Manager opens, as shown in Figure 25 "Service Details" (page 86).

10 From the **Role Mapping** section, in the **Role Name** column, select the check box beside **Subscriber Manager**.

11 Click **Edit Mapping**.

The **Permission Mapping for Subscriber Manager** Web page opens for the selected role, as shown in Figure 26 "Permission Mapping for Subscriber Manager" (page 87).

12 Select a **Permissions** option and click **Save**.

The Services Details Web page opens.

Note: Subscriber Manager appears in the list of Managed Services on the **Services** Web page the next time a user logs on to ECM.

--End--

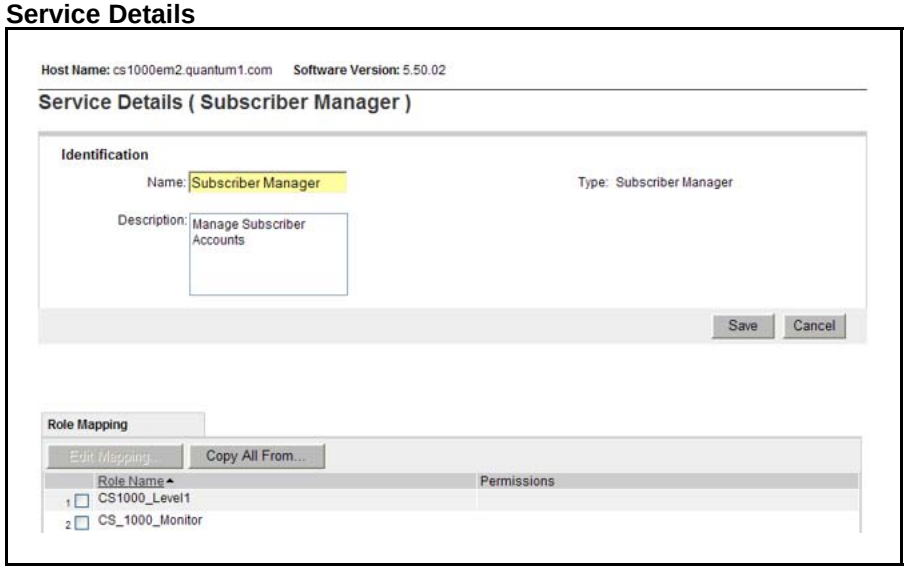
Edit service properties

Use the steps in Procedure 3 “Editing the properties of Subscriber Manager” (page 86) to edit the properties and role-permission mapping of Subscriber Manager.

Procedure 3
Editing the properties of Subscriber Manager

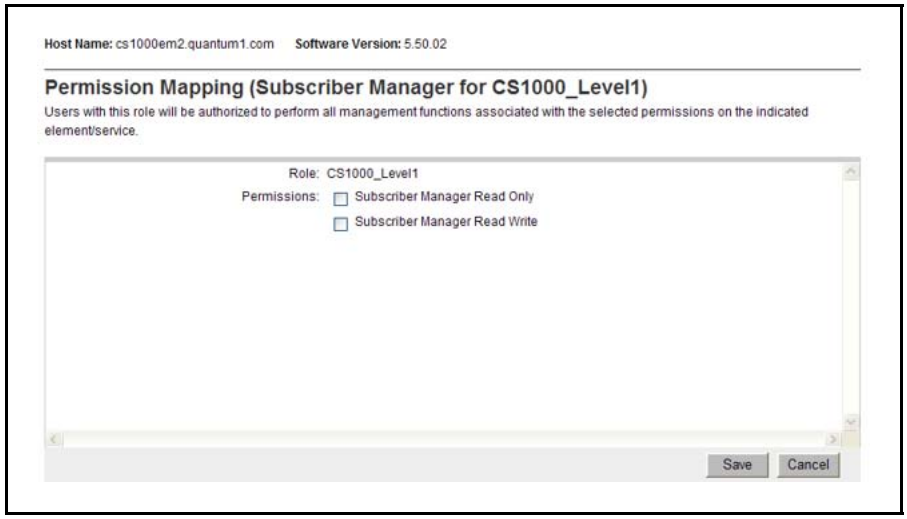
Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Network, Services**. The **Services** Web page opens, as shown in Figure 24 "Services" (page 84).
3	From the **Services** Web page, select the check box beside a service to edit and click **Edit**. The **Service Details** Web page for Subscriber Manager opens, as shown in Figure 25 "Service Details" (page 86).

Figure 25
Service Details



4	In the **Identification** section, edit the following fields as required: • Name • Description
5	From the **Role Mapping** section, in the **Role Name** column, select the check box beside a role. 1. Click **Edit Mapping**. The **Permission Mapping for Subscriber Manager** Web page opens for the selected role, as shown in Figure 26 "Permission Mapping for Subscriber Manager" (page 87).

Figure 26
Permission Mapping for Subscriber Manager



2. Select or clear the permissions for the role and click **Save**.
   The **Service Details** Web page for Subscriber Manager opens, as shown in Figure 25 "Service Details" (page 86).
   Users can select a different role to map permissions to the service.
3. Click **Save**.
   The **Services** Web page opens, as shown in Figure 24 "Services" (page 84).

Or

1. Click **Copy All From**.
   The **Copy element** Web page opens.

   Note: If there are no elements of this type from which to copy, the **Service Details** Web page refreshes displaying an error message.

2. Select an element from the **Copy from Element** drop down list and click **Copy**.
   The **Service Details** Web page for Subscriber Manager opens, as shown in Figure 25 "Service Details" (page 86).
   Users can select a different role to map permissions to the element.
3. Click **Save**.
   The **Services** Web page opens, as shown in Figure 24 "Services" (page 84).

--End--

Security Administration

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.

Navigation

Password

When the user clicks the Password link in the Security branch of the ECM navigation tree, 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.

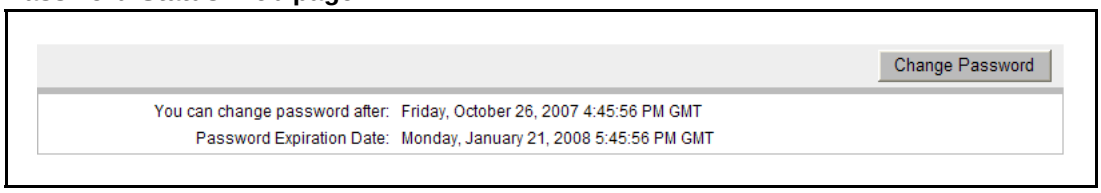
Review the status of a local account password

Use the following procedures to determine when a local password can change and when the password expires.

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 the following figure.

Figure 27
Password Status Web page



ATTENTION
An external user cannot review or change the password.

--End--

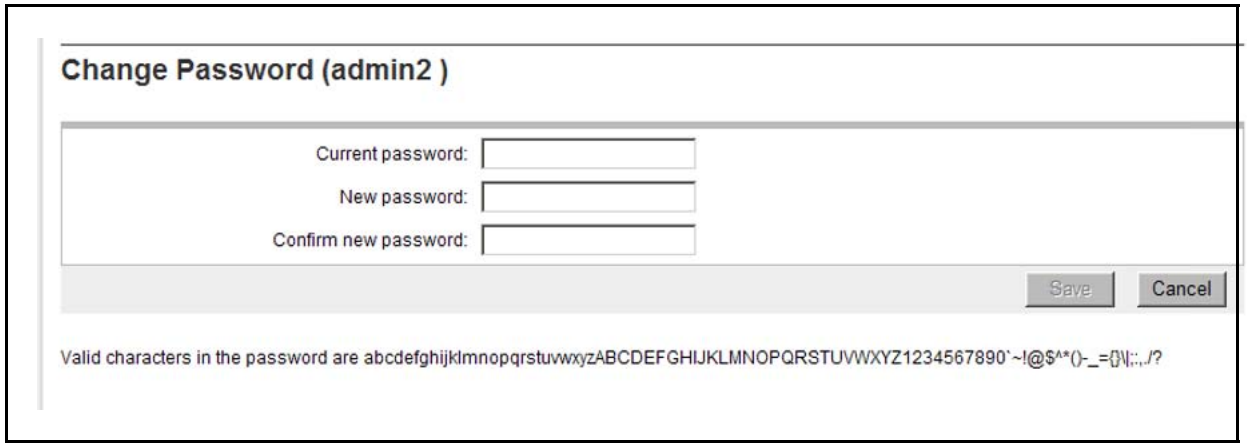
Change a local account password

Use the following procedures to change the current password.

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 27 "Password Status Web page" (page 91).
3	Click **Change Password**. The Change Password Web page appears, as shown in the following figure.

Figure 28
Change Password Web page



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

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

Note: The password must be 50 characters or less.

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 navigation tree, 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.

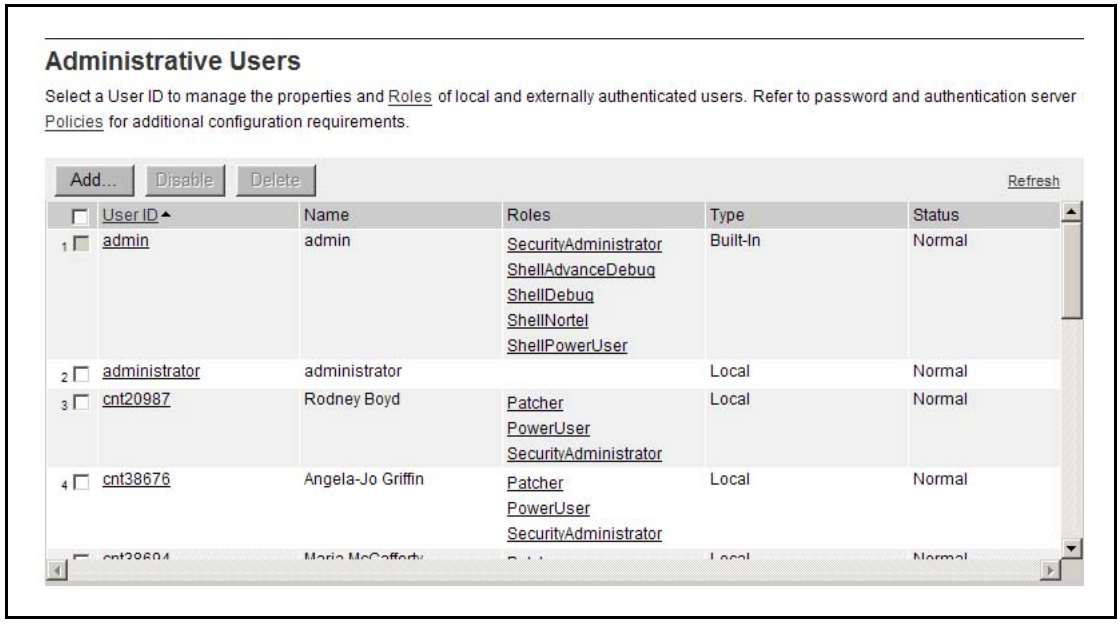
Review existing users

Use the following procedures to view the users that are configured for ECM access.

Reviewing existing users

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page lists users configured for access to ECM. The User ID, name, roles, type, and status are displayed, as shown in the following figure.

Figure 29
Administrative Users Web page



3 Review the information for existing users.

--End--

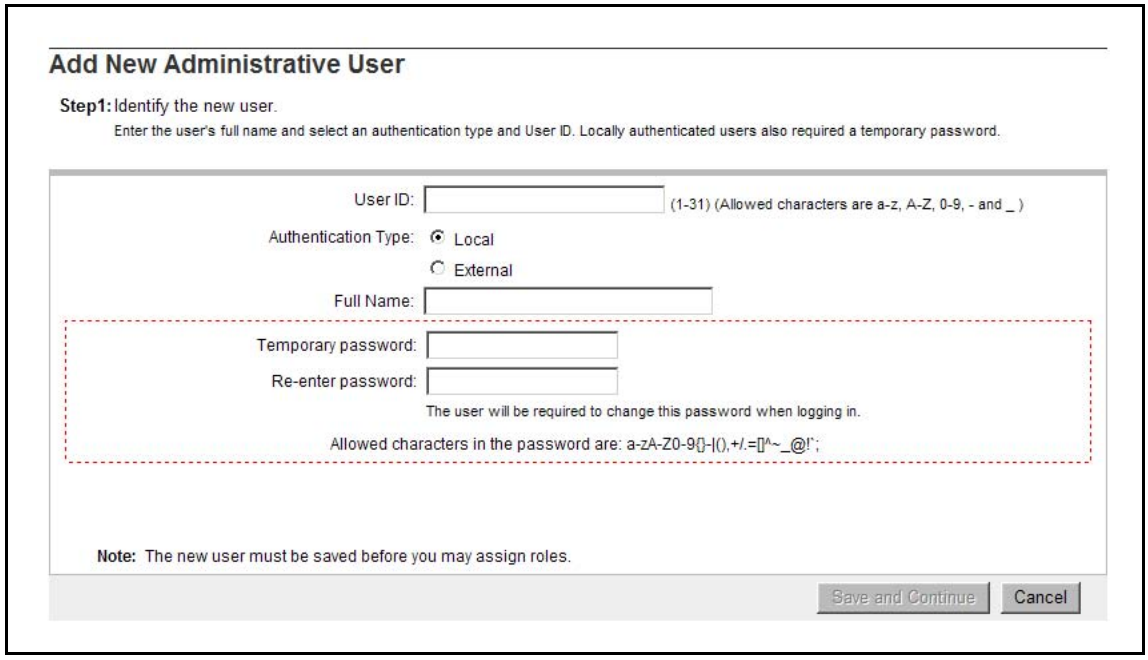
Add a new local or external user

Use the following procedures to create a new user of ECM and to assign roles to the new user. For more information on local and external users, see “Authentication” (page 35).

Adding a new local or external user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
3	Click **Add**. The Add New Administrative User Step 1 Web page appears, as shown in the following figure.

Figure 30
Add New Administrative User Step 1 Web page



4 In the **User ID** field, type the User ID. The User ID can be up to 31 characters in length.

5 From the **Authentication Type**, select **Local** or **External**. For more information on local and external users, see "Authentication" (page 35)

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

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

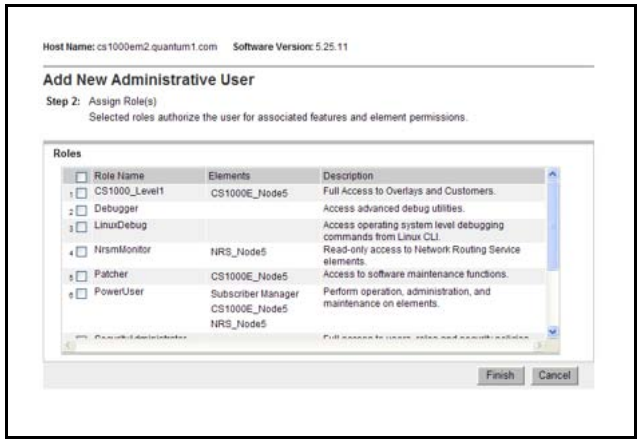
8 In the **Re-enter password** field, type the new password.

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.

9 Click **Save and Continue**.

The Add New Administrative User Step 2 Web page appears, as shown in the following figure.

Figure 31
Add New Administrative User Step 2 Web page



10 Assign roles to the new local user by checking one or more **Role Name** boxes.

11 Click **Finish**.

The Administrative Users Web page opens.

--End--

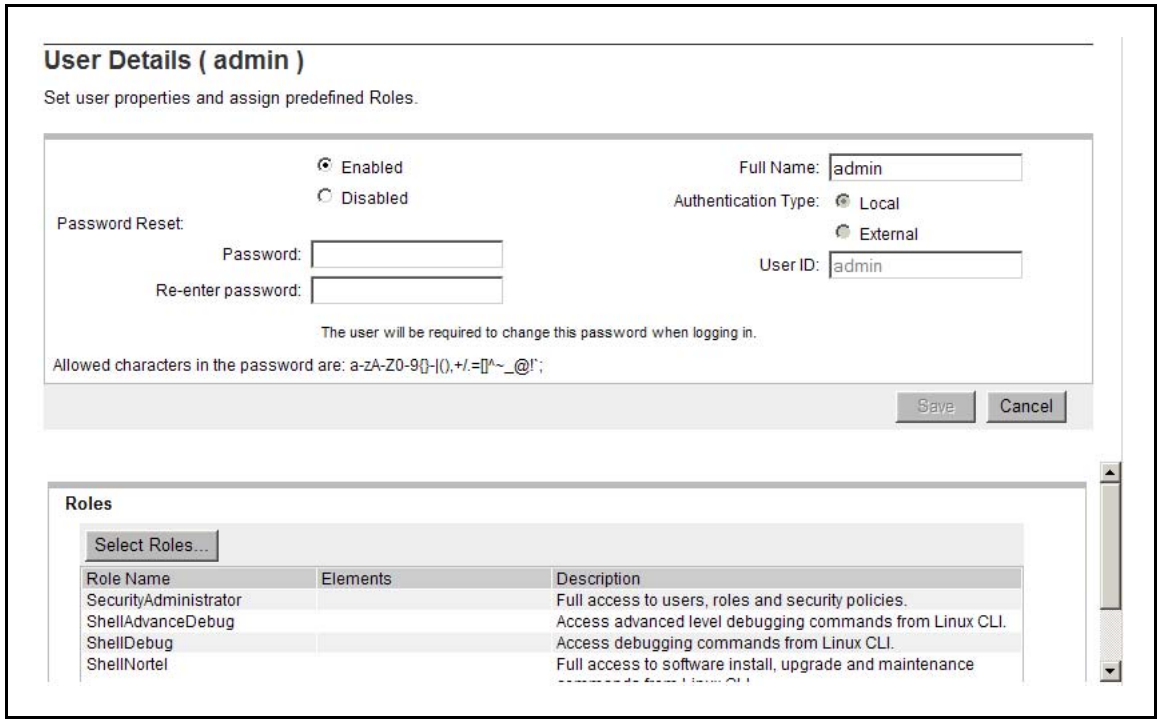
Edit user role mapping

Use the following procedures to select roles to authorize a user for associated features and element permissions.

Editing user role mapping

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
3	Click the name of a user to edit the user role mapping. The User Details Web page appears, as shown in the following figure.

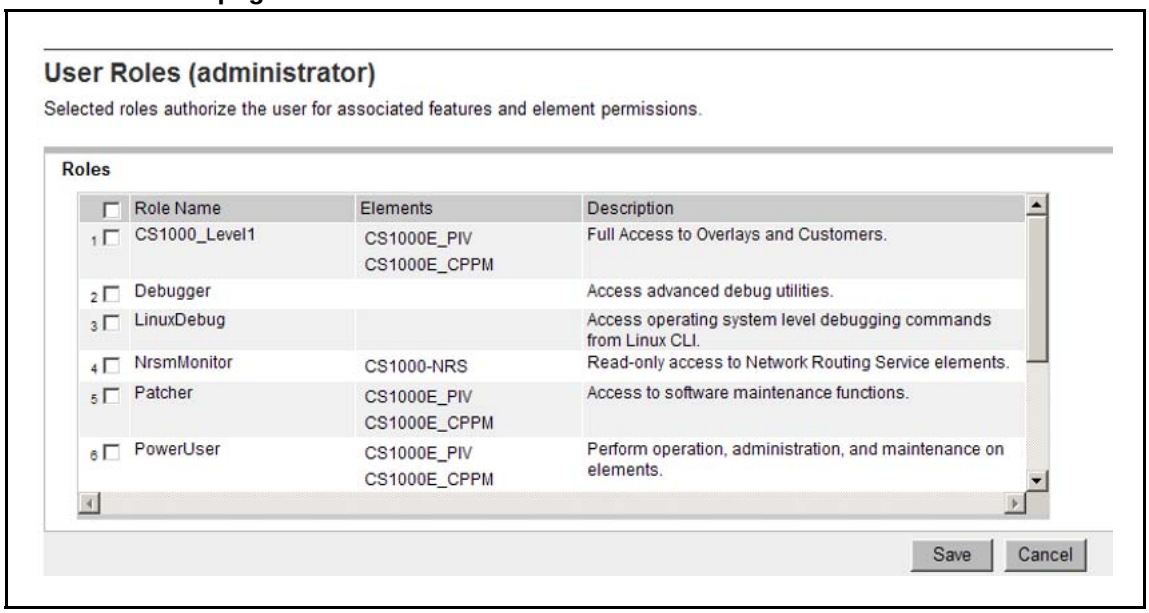
Figure 32
User Details Web page



4 Click **Select Roles**.

The User Roles Web page appears for the selected user, as shown in the following figure.

Figure 33
User Roles Web page



5 Select or deselect the roles for the selected user.

6 Click **Save**.

The **User Details** Web page appears, as shown in Figure 32 "User Details Web page" (page 96).

--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 password and full name for a local user, to disable and enable a local user account, and to delete a user.

Edit the password and full name for a local user account

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

Editing the password and 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** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
3	Click the name of the user. The **User Details** Web page appears, as shown in Figure 32 "User Details Web page" (page 96).
4	(Optional.) In the **Full Name** field, edit the name of the user.
5	In the **Password Reset** section, in the **Password** field, enter a new password.
6	In the **Re-enter password** field, type the new password again. ***Note:*** There will be a prompt to reset the new password the first time the user logs on to ECM.
7	Click **Save**.

The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).

--End--

Disable a user account

Use the following procedures to disable a user account within ECM.

Disabling a user account

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
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 following procedures to enable a user account within ECM.

Enabling a user account

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
3	Click the user ID for the disabled user account. The User Details Web page appears, as shown in Figure 32 "User Details Web page" (page 96).
4	From the **User Details** Web page, select **Enabled**.

5 In the **Password Reset** section, in the **Password** field, type a new password.

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

Note: There will be a prompt to reset the new password the first time the user logs on to ECM.

7 Click **Save**.

--End--

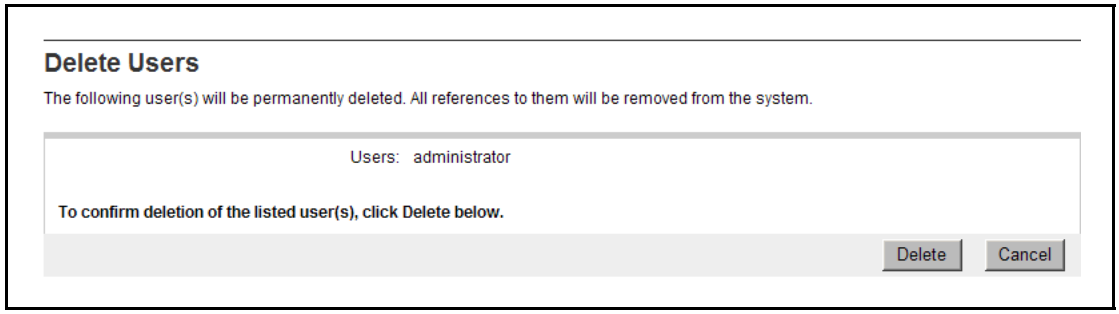
Delete a user

Use the following procedures to delete one or more users in ECM.

Deleting a user

Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 29 "Administrative Users Web page" (page 93).
3	Click the check box beside the name(s) of one or more user(s).
4	Click **Delete**. The Delete Users Web page appears, as shown in the following figure.

Figure 34
Delete Users Web page



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 navigation tree, 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.

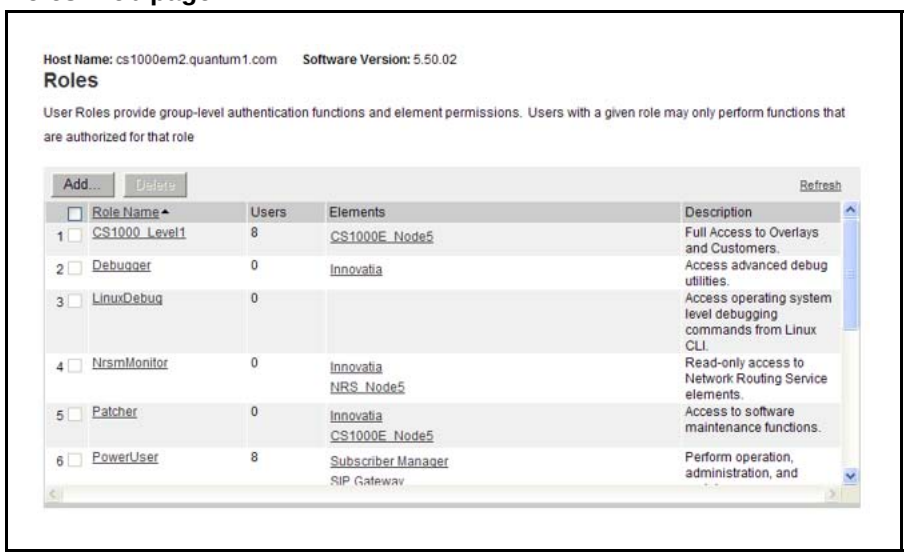
Review existing roles

Use the following procedures to view the current roles in ECM.

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 the following figure.

Figure 35
Roles Web page



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

--End--

Add a new role

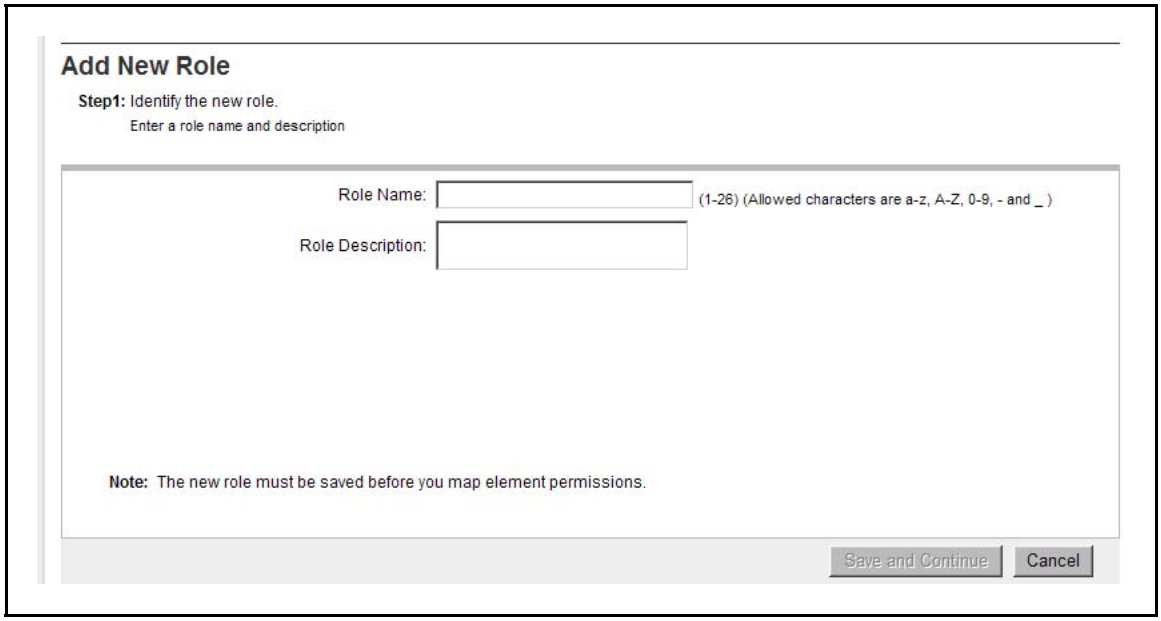
A security administrator can add new roles to the default list of roles currently in ECM to manage access control for users of their management system.

Use the following procedures to add a new role for specific access control policies in ECM.

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 35 "Roles Web page" (page 100).
3	Click **Add**. The Add New Role Step 1 Web page opens, as shown in the following figure.

Figure 36
Add New Role Step 1



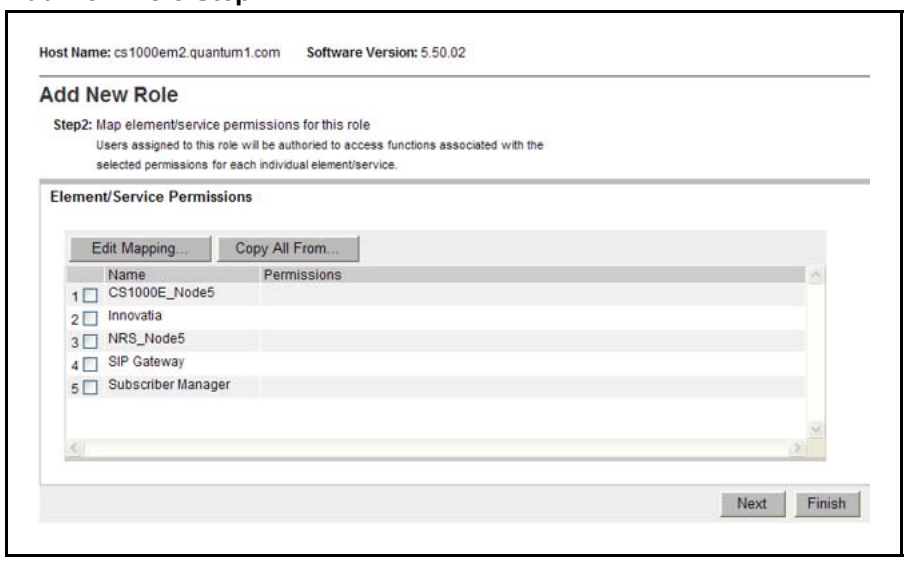
4 In the **Role Name** field, type the unique role name.

5 In the **Role Description** field, type a description for the new role.

6 Click **Save and Continue**.

The Add New Role Step 2 Web page opens, as shown in the following figure.

Figure 37
Add New Role Step 2

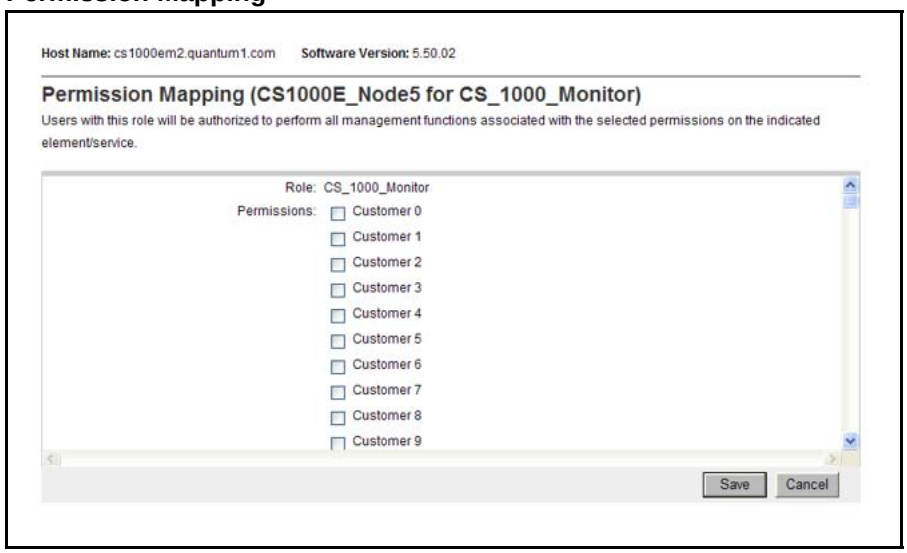


7 Select a check box beside an element Name.

8 Click **Edit Mapping** to map element/service permission for this role.

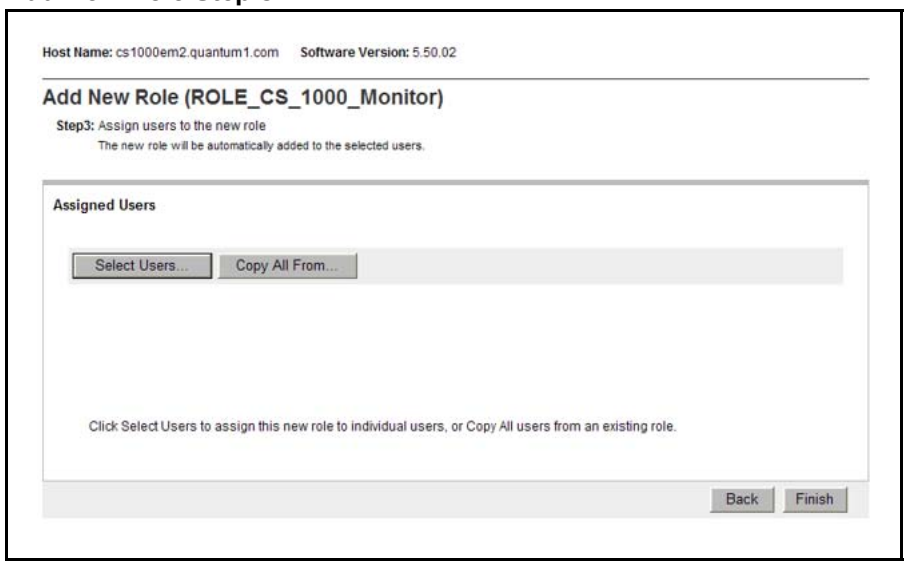
The Permission Mapping Web page opens, as shown in the following figure.

Figure 38
Permission Mapping



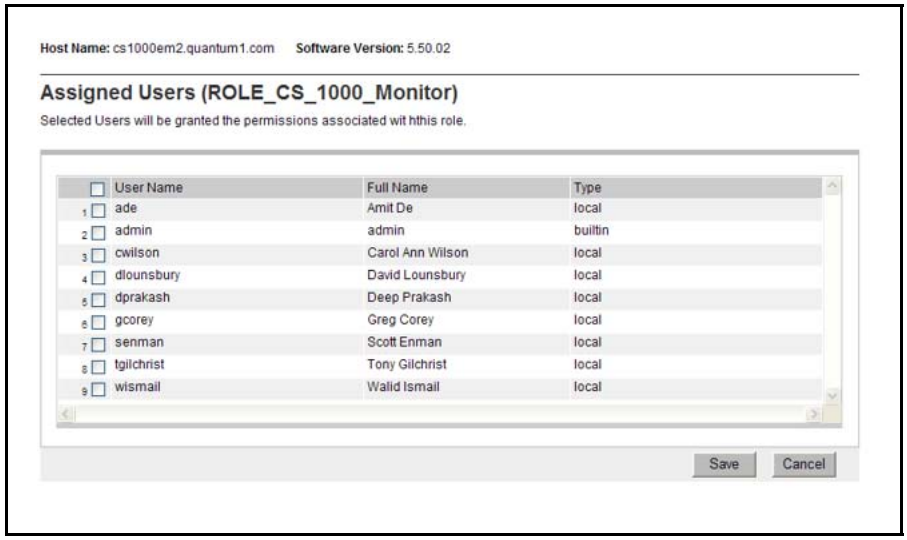
- Assign permission for this role by selecting one or more check boxes.
- Click **Save**.
  The Add New Role Step 2 Web page opens, as shown in the following figure.
- Click **Next.**
  The Add New Role Step 3 Web page opens, as shown in the following figure.

Figure 39
Add New Role Step 3



1. Click **Select Users** to assign this new role to individual users.
   The Assigned Users Web page opens, as shown in the following figure.

Figure 40
Assigned Users

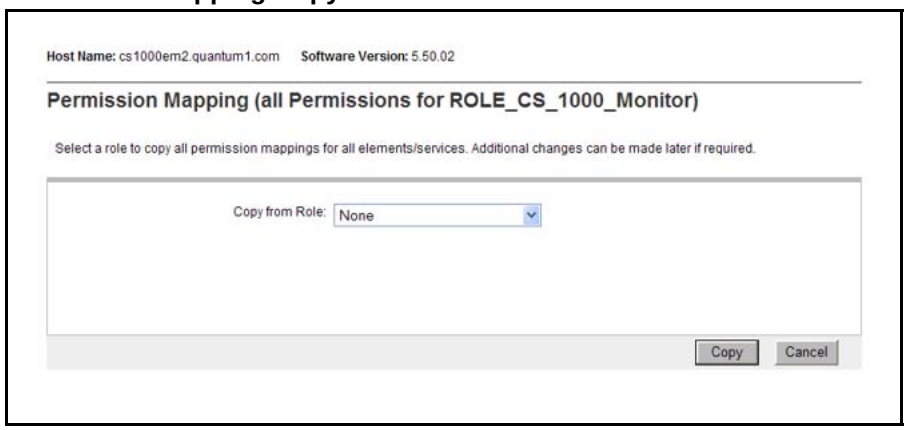


2. Select one or more check boxes beside the User Name to grant permissions associated with this role.
3. Click **Save**.
   The Add New Role Step 3 Web page opens, as shown in Figure 39 "Add New Role Step 3" (page 103).
4. Click **Finish**.
   The Roles Web page opens, as shown in Figure 35 "Roles Web page" (page 100).

Or

1. Click **Copy All From** to duplicate a list of users assigned to another role.
   The Permission Mapping Copy from Role Web page opens, as shown in the following figure.

Figure 41
Permission Mapping Copy from Role



2. Select a role from the **Copy from Role** list.

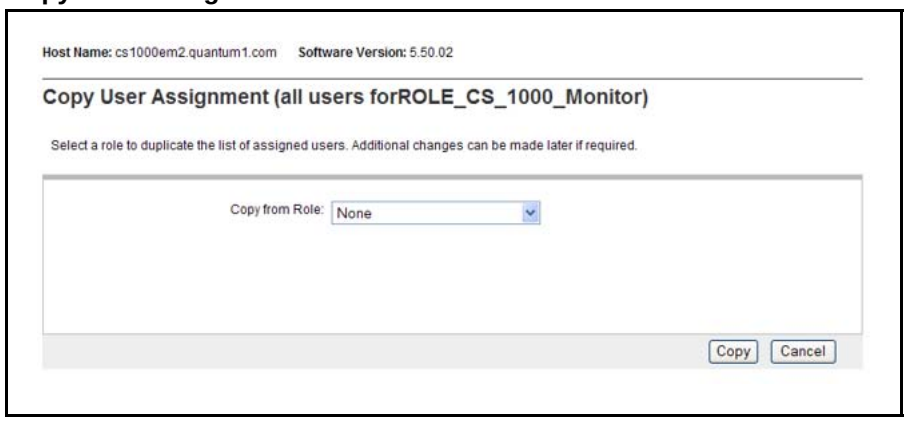
3. Click **Copy**.
   The Add New Role Step 2 Web page opens, as shown in Figure 37 "Add New Role Step 2" (page 102).
4. Click **Finish**.
   The Roles Web page opens, as shown in Figure 35 "Roles Web page" (page 100).

9 Or

Click **Copy All From** to duplicate a list of users assigned to another role.

The Copy User Assignment Web page opens, as shown in the following figure.

Figure 42
Copy User Assignment



1. Select a role from the **Copy from Role** list.
2. Click **Copy**.
   The Add New Role Step 3 Web page opens, as shown in Figure 39 "Add New Role Step 3" (page 103).
3. Click **Finish**.
   The Roles Web page opens, as shown in Figure 35 "Roles Web page" (page 100).

--End--

Edit a role description

Use the following procedures to change the description for a role in ECM.

Editing a role description

Step	Action
1	Log on to ECM.

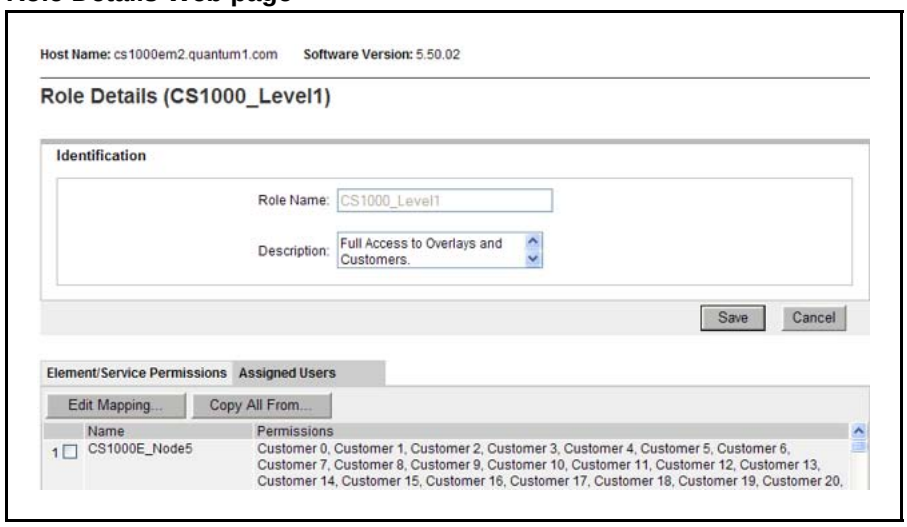
2 From the navigation pane, click **Security** , **Roles**.

The Roles Web page appears, as shown in Figure 35 "Roles Web page" (page 100).

3 From the **Role Name** column, click a Role Name to edit the description.

The Role Details Web page appears, as shown in the following figure.

Figure 43
Role Details Web page



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

5 Click **Save**.

The Roles Web page appears, as shown in Figure 35 "Roles Web page" (page 100).

--End--

Edit role user mapping

Use the following procedures to select users to grant the permissions associated with a selected role.

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 35 "Roles Web page" (page 100).

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

The Role Details Web page appears as shown in Figure 43 "Role Details Web page" (page 106).

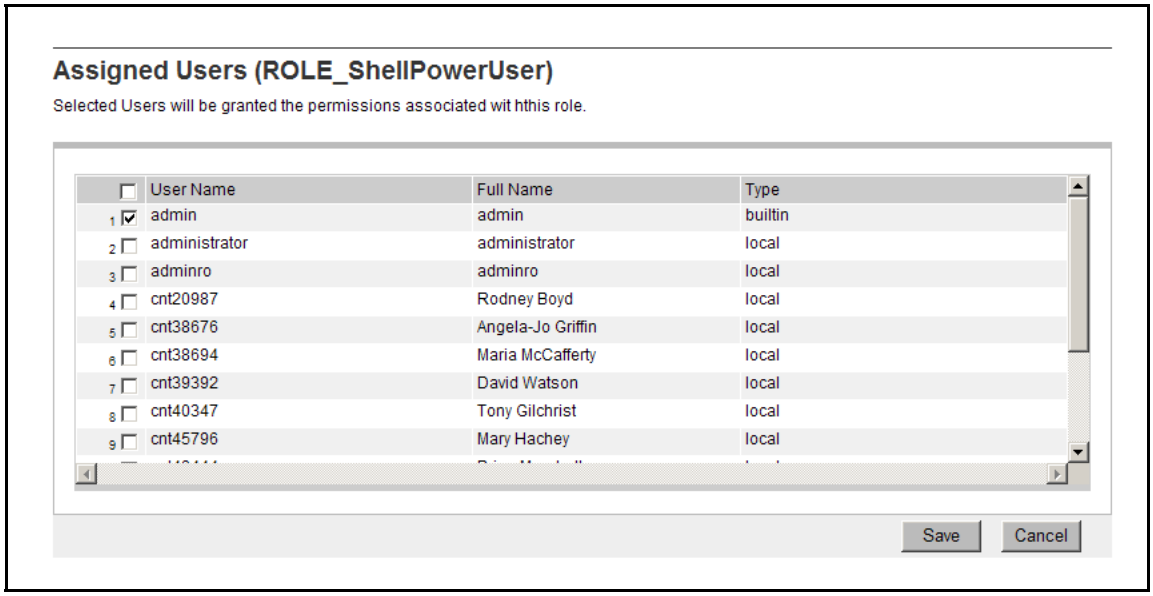
4 Click **Assigned Users**.

The Role Details Web page refreshes with a list of users granted the permissions associated with the selected role.

5 Click **Select Users**.

The Assigned Users Web page for the selected role appears, as shown in the following figure.

Figure 44
Assigned Users Web page



6 Select the users to be granted the permissions associated with the selected role. To remove permissions for a User Name, clear the check box.

7 Click **Save**.

The Role Details Web page appears. as shown in Figure 43 "Role Details Web page" (page 106).

--End--

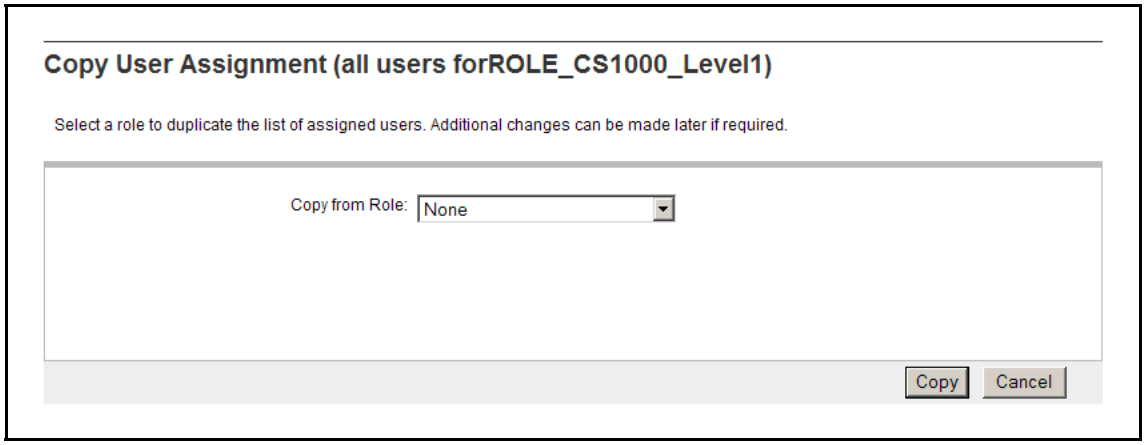
Copy all users from role

Use the following procedure to select a role to copy the list of assigned users.

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 35 "Roles Web page" (page 100).
3	From the **Role Name** column, click a role name. The Role Details Web page appears as shown in Figure 43 "Role Details Web page" (page 106).
4	Click **Assigned Users**. The Assigned Users Web page for the selected role appears, as shown in Figure 44 "Assigned Users Web page" (page 107)
5	Click **Copy All From**. The Copy User Assignment Web page appears, as shown in the following figure.

Figure 45
Copy User Assignment Web page



6	Select a role from the **Copy from Role** list, and click **Copy**. The Role Details Web page appears as shown in Figure 43 "Role Details Web page" (page 106).

--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.

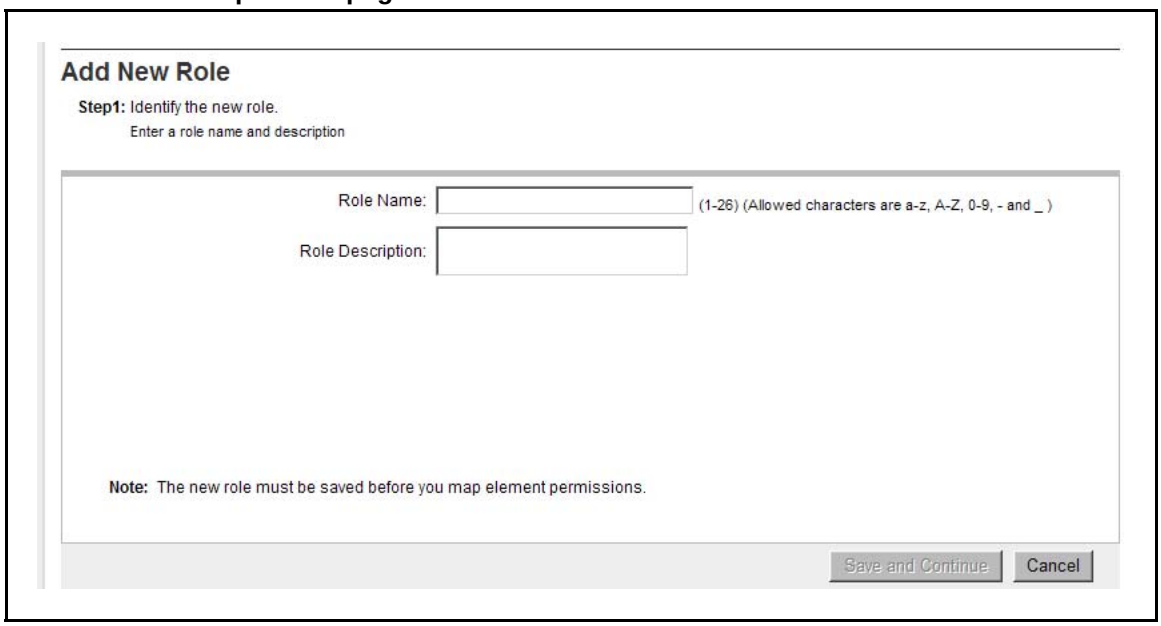
Edit role element permissions with Edit Mapping for a new role

Use the following procedure to edit role element permissions with Edit Mapping for a new role in ECM.

Editing role element permissions with Edit Mapping for a new role

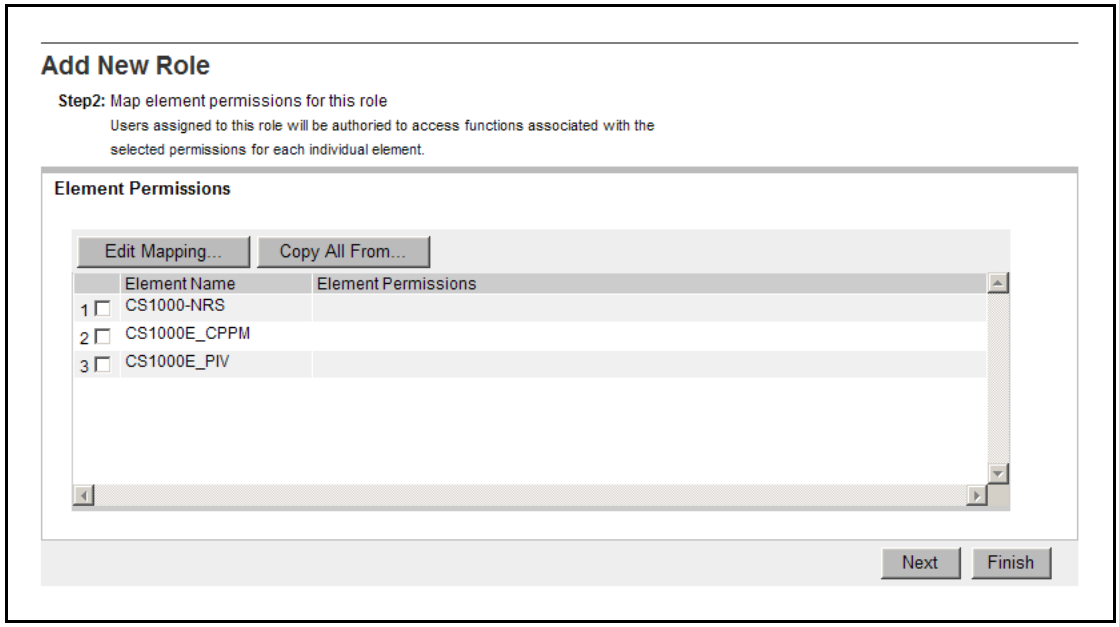
Step	Action
1	Log on to ECM as a security administrator.
2	From the navigation pane, click **Security** , **Roles**. The Roles Web page appears, as shown in Figure 35 "Roles Web page" (page 100).
3	Click **Add**. The Add New Role Step 1 Web page appears, as shown in the following figure.

Figure 46
Add New Role Step 1 Web page



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 the following figure.

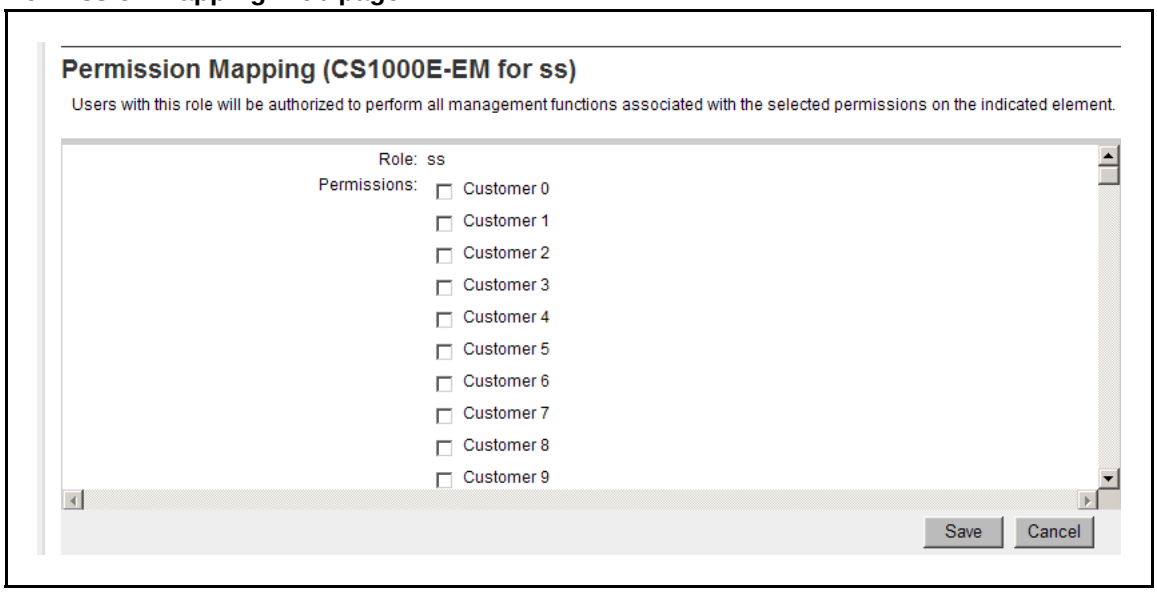
Figure 47
Add New Role Step 2 Web page



5 From the **Add New Role Step 2** Web page, in the **Element Permissions** 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 the following figure.

Figure 48
Permission Mapping Web page



6 From the **Permissions** list, select the check box beside the desired permissions for the selected element for the new role.

ATTENTION
When mapping permissions for a CS 1000 element, ensure the **Print Routine 3** permission is selected; otherwise, users cannot log on to the CS 1000 element.

7 Click **Save**.

--End--

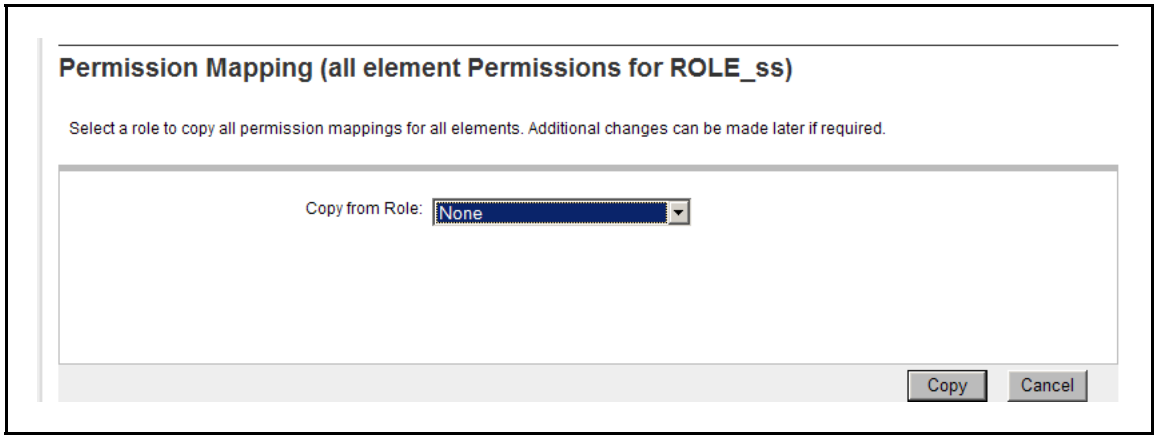
Edit role element permissions with Copy All From for a new role

Use the following procedure to edit role element permissions with Copy All From for a new role in ECM.

Editing role element permissions with Copy All From for 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 35 "Roles Web page" (page 100)
3	Click **Add**. The Add New Role Step 1 Web page appears as shown in Figure 46 "Add New Role Step 1 Web page" (page 109).
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 47 "Add New Role Step 2 Web page" (page 110).
5	From the **Add New Role Step 2** Web page, in the **Element Permissions** section, click **Copy All From**, as shown in Figure 47 "Add New Role Step 2 Web page" (page 110). The Permission Mapping Web page appears, as shown in the following figure.

Figure 49
Permission Mapping, Copy from Role Web page



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

7 Click **Copy**.

The Add New Role Step 2 Web page appears.

8 Click **Finish**.

--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 following procedure to edit a role element permission using Edit Mapping.

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 35 "Roles Web page" (page 100).
3	From the **Role Name** column, click a Role Name to edit the permissions. The Role Details Web page appears, as shown in Figure 43 "Role Details Web page" (page 106).
4	Select a check box beside an element **Name**.

5 Click **Edit Mapping** to edit the element/service permission mapping for this role.

The Permission Mapping Web page opens, as shown in Figure 38 "Permission Mapping" (page 102).

6 Select the check box to assign permissions associated with this role. To remove permissions, clear the check box.

7 Click **Save**.

The Role Details Web page appears, as shown in Figure 43 "Role Details Web page" (page 106).

--End--

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

Use the following procedure to edit a role element permission using Copy All From.

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 35 "Roles Web page" (page 100).
3	From the **Role Name** column, click a Role Name to edit the permissions. The Role Details Web page appears as shown in Figure 43 "Role Details Web page" (page 106).
4	Select a check box beside an element **Name**.
5	Click **Copy All From** to edit the element/service permission mapping for this role. The **Permission Mapping** Web page appears, as shown in Figure 49 "Permission Mapping, Copy from Role Web page" (page 112).
6	From the **Copy from Role** list, select a role to copy from.
7	Click **Copy**. The Role Details Web page appears as shown in Figure 43 "Role Details Web page" (page 106).

8	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.

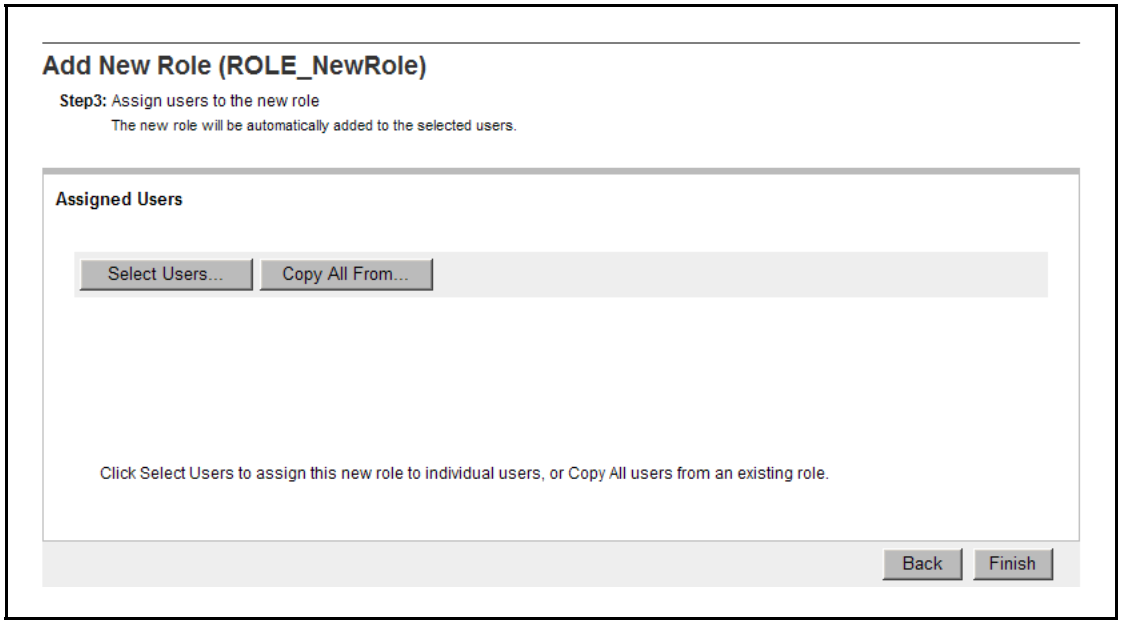
Edit a role user assignment when adding a new role with Select Users

Use the following procedures to edit a role user assignment with select users.

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 35 "Roles Web page" (page 100).
3	Click **Add**. The Add New Role Step 1 Web page appears, as shown in Figure 46 "Add New Role Step 1 Web page" (page 109).
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 47 "Add New Role Step 2 Web page" (page 110).
5	Click **Next**. The Add New Role Step 3 Web page opens, as shown in the following figure.
6	Click **Select Users**.

Figure 50
Add New Role Step 3



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

7 Click **Save**.

The Add New Role Step 3 Web page opens.

8 Click **Finish**.

--End--

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

Use the following procedure to edit a role user assignment using Copy All From.

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 35 "Roles Web page" (page 100)
3	Click **Add**. The Add New Role Step 1 Web page appears, as shown in Figure 46 "Add New Role Step 1 Web page" (page 109).

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 47 "Add New Role Step 2 Web page" (page 110).

5 Click **Next**.

The Add New Role Step 3 Web page opens, as shown in Figure 50 "Add New Role Step 3" (page 115).

6 Click **Copy All From**.

7 Select an element to copy from.

8 Click **Copy**.

The Add New Role Step 3 Web page opens.

9 Click **Finish**.

--End--

Delete custom roles

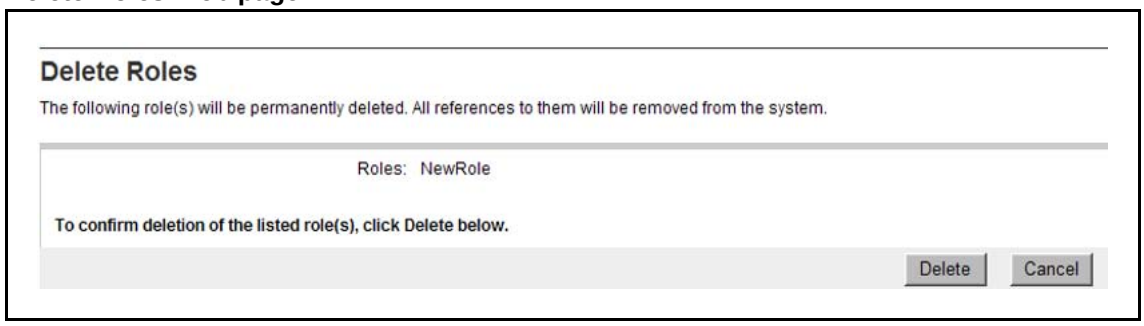
Use the following procedure to delete custom roles.

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.

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 the following figure.

Figure 51
Delete Roles Web page



4 Click **Delete** 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 navigation tree, 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

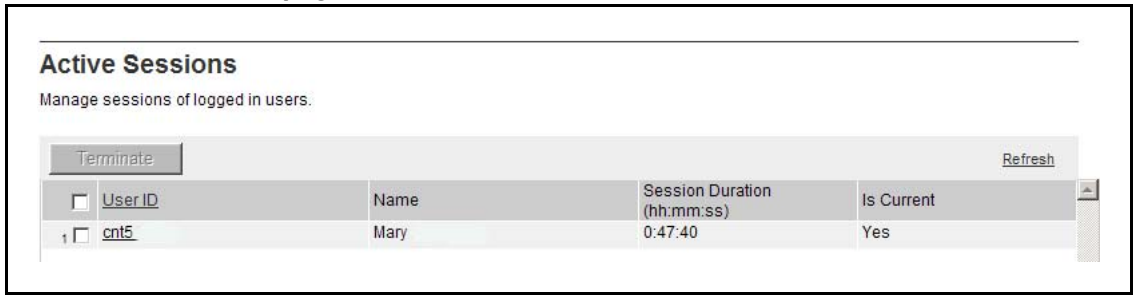
Security administrators can see all users who are currently logged on to ECM and view the session time for the user.

Use the steps in "Viewing active sessions" (page 117) to view the current sessions in ECM.

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 the following figure. The sessions are sorted in the **User ID** column.

Figure 52
Active Sessions Web page



--End--

Terminate Single Sign-On sessions

Use the following procedure to terminate selected Single Sign-On (SSO) sessions in ECM.

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 52 "Active Sessions Web page" (page 117).
3	Select the required sessions to terminate.
4	Click **terminate**. 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 navigation tree, 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 and the SSO cookie domain.

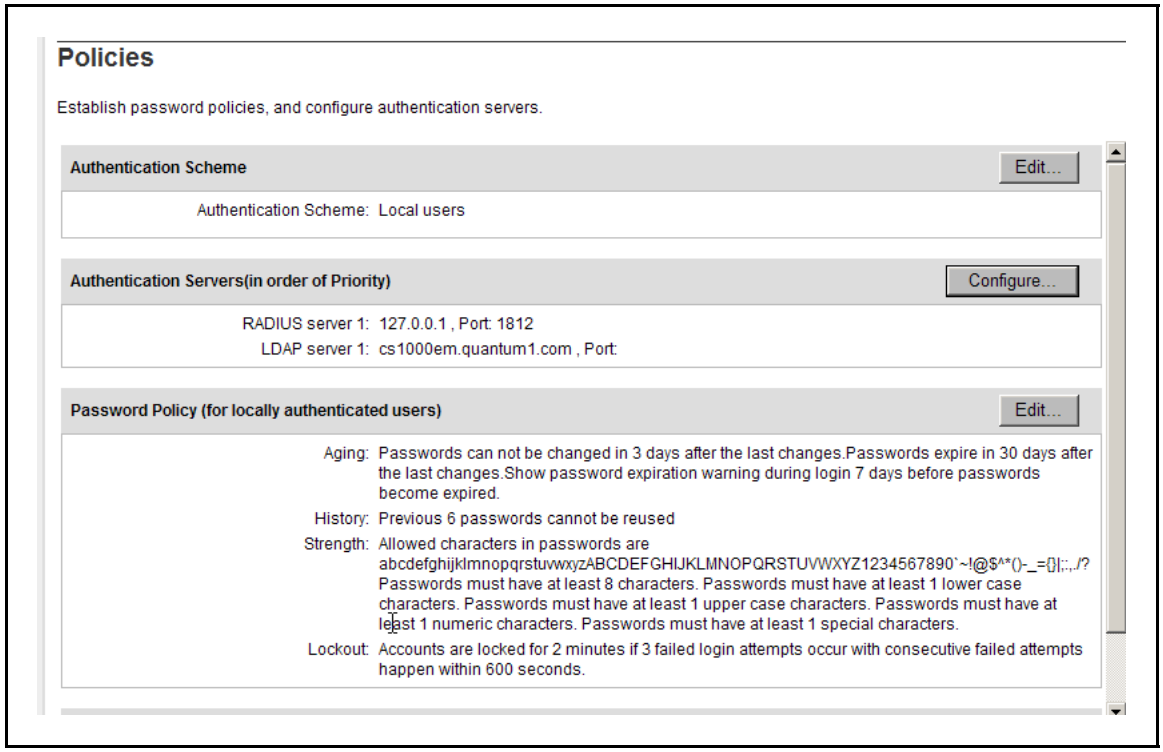
Review security policies

Use the following procedure to review the currently configured security policies within the ECM.

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

Figure 53
Policies Web page



--End--

Edit the authentication scheme

Use the steps in "Editing the authentication scheme" (page 120) to edit the authentication scheme. ECM supports up to three authentication authorities:

- local users
- external RADIUS users
- external LDAP users

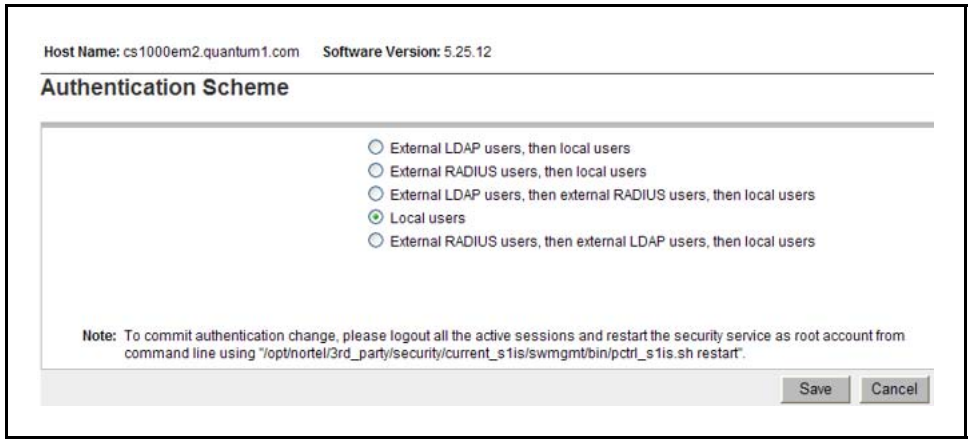
The authentication scheme policy determines the order that the three authentication authorities are used. The supported orders in ECM are as follows:

- 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.

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 53 "Policies Web page" (page 119).
3	From the **Policies** Web page, in the **Authentication Scheme** section, click **Edit**. The Authentication Scheme Web page appears, as shown in the following figure.

Figure 54
Authentication Scheme Web page



Step	Action
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."

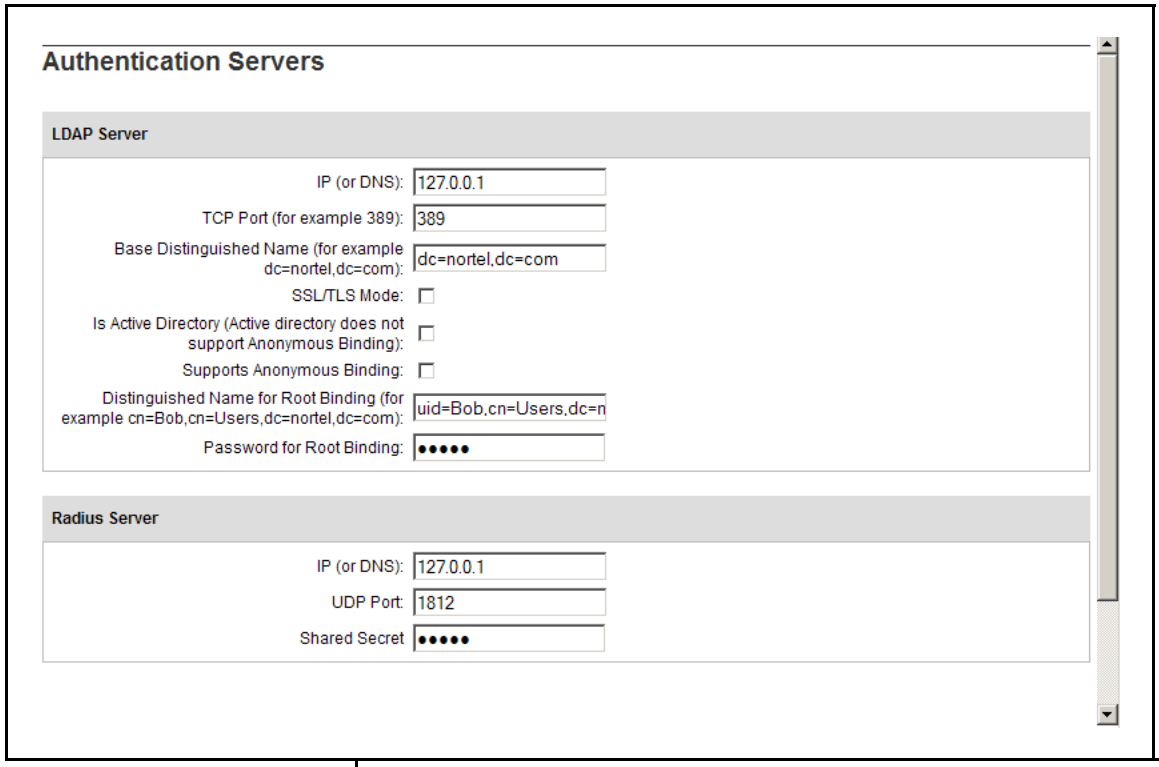
Configure the LDAP authentication server

Use the following procedures to complete the required information for the LDAP authentication server.

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 53 "Policies Web page" (page 119).
3	From the **Policies** Web page in the **Authentication Servers** section, click **Configure**. The Authentication Servers Web page appears, as shown in Figure 55 "Authentication Servers Web page" (page 122).
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 **TCP Port** field, type the TC port number of the LDAP server. • In the **Base Distinguished Name** field, type 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 55
Authentication Servers Web page



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 following procedure to complete the required information for the RADIUS authentication server.

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 53 "Policies Web page" (page 119). 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 55 "Authentication Servers Web page" (page 122).

4 In the **RADIUS Server**, complete 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--

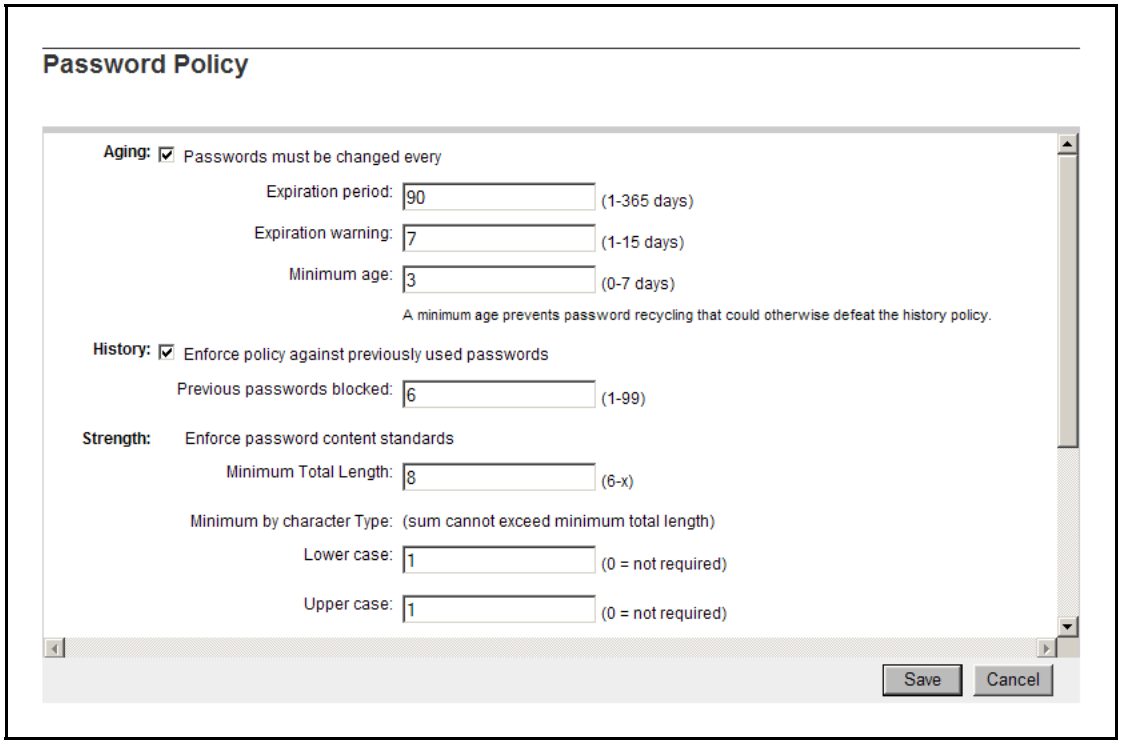
Edit local account password policies

Use the following procedure to configure the local account password policies including, aging, history, strength, and lockout password policies in ECM according to business requirements.

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 53 "Policies Web page" (page 119).
3	From the Policies Web page in the **Password Policy** section, click **Edit**, as shown in Figure 53 "Policies Web page" (page 119). The Password Policy Web page appears, as shown in the following figure.

Figure 56
Password Policy Web page



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 "Resetting a user password from the CLI" (page 46).

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 logon attempt is made on a disabled account.
- The password is invalid.
- The maximum number of log on attempts has been reached.
- The password is 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 a failed log on attempt is reached.

The system sends a warning message when a password is about to expire. The password must be changed.

8 Click **Save**.

--End--

Edit the SSO cookie domain

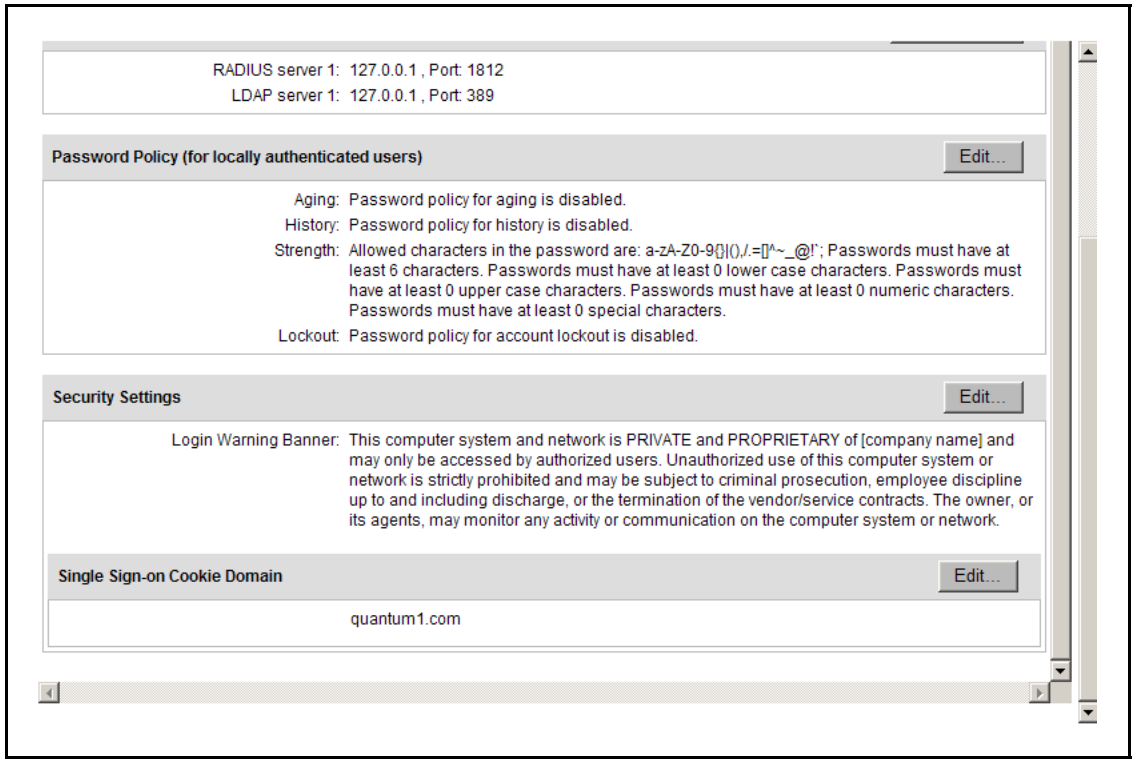
When the primary and backup security servers are configured in different domains, SSO requires authentication to switch from the primary to backup security server. For authentication, the primary and backup security server domain names must match.

Use the following procedure to change the SSO cookie domain.

Procedure 4
Editing the SSO cookie domain

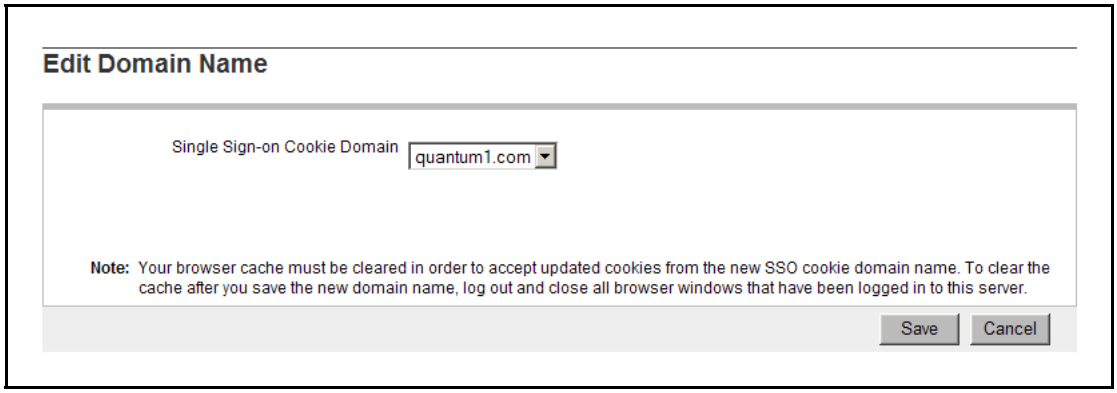
Step	Action
1	Log on to the ECM framework as a security administrator.
2	In the navigation pane, click **Security** , **Policies**. The Policies Web page appears, as shown in Figure 57 "Policies Web page" (page 127).
3	From the **Policies** Web page, in the **Single Sign-On Cookie Domain** section, click **Edit**, as shown in the following figure.

Figure 57
Policies Web page



The Edit Single Sign-On Cookie Domain Web page appears, as shown in the following figure.

Figure 58
Edit Single Sign-On Cookie Domain Web page



4 From the **Single Sign-On Cookie Domain** list, select a URL to change the SSO cookie domain.

5 Click **Save** to save the change or **Cancel** to discard the change.

--End--

ATTENTION
When the SSO cookie domain is changed, users must clear the existing ECM related cookies from the cache in the Internet browser for all users.

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 the following figure.

Table 17
Default Login warning message

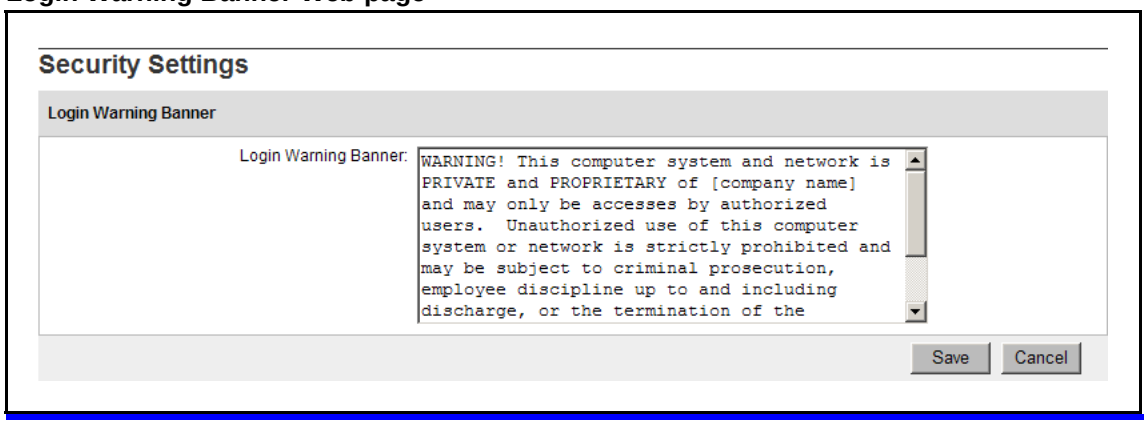
WARNING! This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, 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 following procedure to customize the message for the login warning banner in ECM.

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 53 "Policies Web page" (page 119).
3	From the **Policies** Web page in the **Security Settings** section, click **Edit**. The **Login Warning Banner** Web page appears, as shown in the following figure.

Figure 59
Login Warning Banner Web page



4 In the **Login Warning Banner** text area, edit the text as required.

5 Click **Save**.

--End--

Tools

This chapter contains information on the Tools branch in the Enterprise Common Manager (ECM) navigation pane.

Navigation

Logs

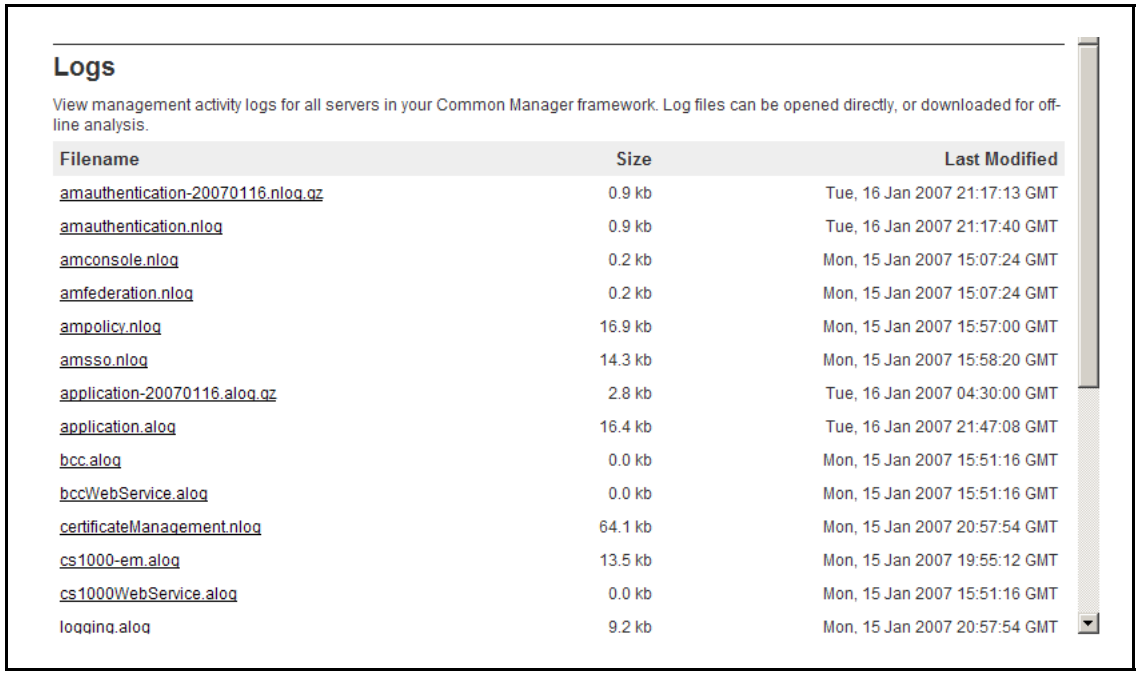
When the user clicks the Logs link in the Tools branch of the ECM navigation tree, the Logs Web page appears. From the Logs Web page, a security administrator can review or download log files.

Use the steps in "Reviewing log files" (page 131) to review management activity logs in the current or a new Web browser window or to download a log file.

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 the following figure.

Figure 60
Directory Listing For logs Web page



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 navigation tree, 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 following procedure to view the current status for SNMP.

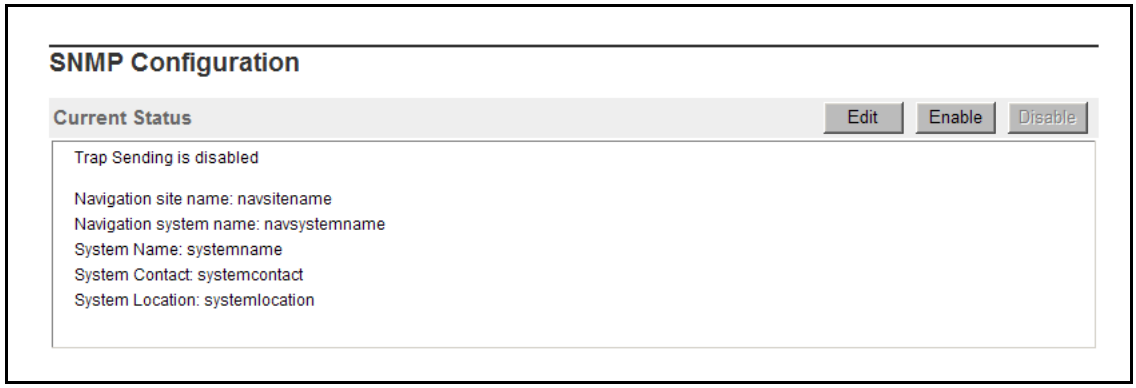
Viewing the status of SNMP

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 61 "SNMP Web page" (page 133).

Figure 61
SNMP Web page



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

--End--

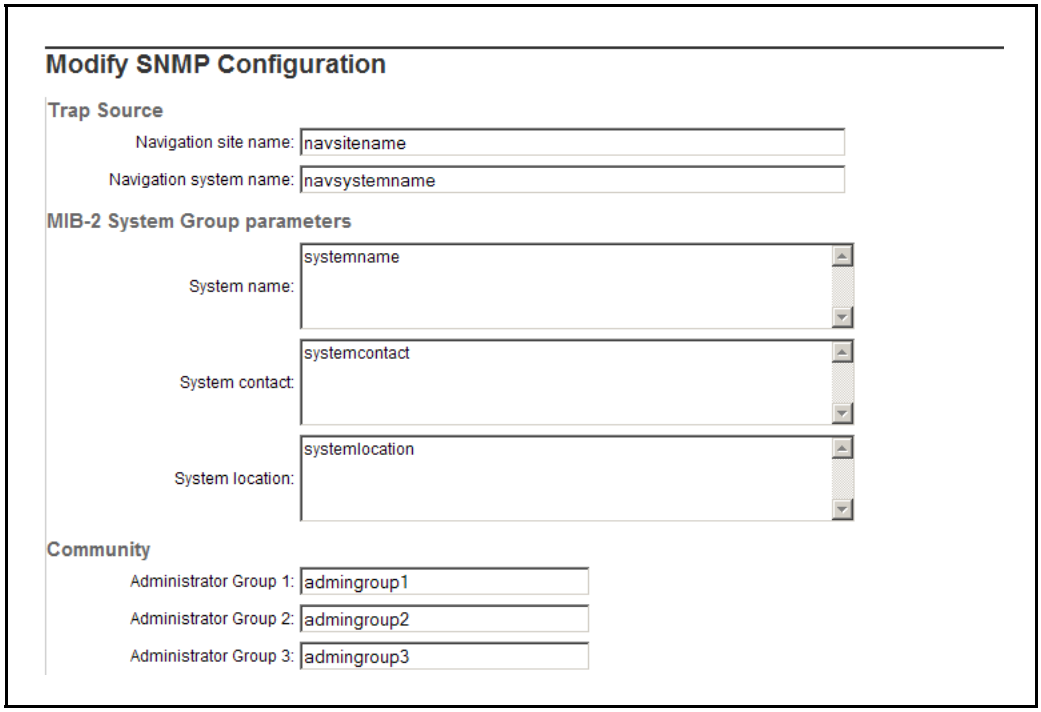
Modify the SNMP configuration

Use the following procedure to modify the SNMP configuration.

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 61 "SNMP Web page" (page 133).
3	Click **Edit**. The Modify SNMP Configuration Web page appears, as shown in the following figure.

Figure 62
Modify SNMP Configuration Web page



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 following procedure to enable or disable trap sending for SNMP configuration in ECM.

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 61 "SNMP Web page" (page 133).
3	From the SNMP Web page, click **Enable Trap** or **Disable Trap** to enable or disable trap sending.

--End--

Upgrade

This chapter contains information on upgrading an ECM application.

ATTENTION
Before upgrading an ECM application ascertain whether the Linux base has to be upgraded. If the Linux base has to be upgraded, install both the upgraded Linux base and the upgraded ECM application. For information about installing Linux and the ECM applications, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*. To upgrade the ECM applications without upgrading the Linux base use the procedures described in this chapter.

Navigation

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 "Upgrading the ECM primary and backup security service on a Linux server" (page 138) to upgrade the current ECM primary and backup security service on a Linux server.

ATTENTION
User has to deconfig the HA setup before re-installation of Backup Security Server.

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 following procedure to upgrade the current ECM security member server.

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 following procedure to reinstall the ECM security service applications on a Linux server.

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 information on backup and restore.

Navigation

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/nortel
- data from security service

ATTENTION
The ECM data can be backed up by performing a system backup of the Linux base and applications by using the Linux base CLI command **`sysbackup`**, or the ECM data only can be backed up by using the procedures described in this chapter. For more information on Linux base CLI commands see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

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>
```

A successful restore operation can be performed only once with a given backup file.

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 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 following procedure 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`.

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

Step	Action
1	From the command line interface, 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.
5	Use the Linux base CLI command hostconfig to enter the new IP address for FQDN mapping.
6	Enter the FQDN mapping in the DNS server or in the PC Web client `C:\WINNT\system32\drivers\etc\hosts`.

ATTENTION
Use the CLI command hostconfig 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:7
b: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
Use the CLI command hostconfig 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, log on as root user and use the Linux base CLI command **networkconfig** to change the IP address of eth0. For more information about Linux base CLI commands, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Modify the FQDN of the security member server

Use the following procedure 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.

Modifying the FQDN of the security member server

Step	Action
1	Change the host name and FQDN of the member server through baseparamsconfig.
2	Use the Linux base CLI command hostconfig to enter the new IP address for FQDN mapping.

3 Enter the FQDN mapping in the DNS server or in the PC Web client **C:\WINNT\system32\drivers\etc\hosts**.

ATTENTION
Use the CLI command hostconfig in all the Linux servers if the DNS server is not used.

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

--End--

Appendix Linux root account command line interface commands

Table 18 "Linux root account CLI commands" (page 149) 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 18
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 Manager Web server.	cat /opt/sun/Webserver/https-oamplatform/log s/errors

Appendix 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.

The following table shows the least privilege algorithm for Tom.

Table 19
Least privilege algorithm

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

Appendix 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.

The following table shows the permission assignment for the roles in ABC company.

Table 20
Permission assignment for the roles in ABC company

Role Name CS 1000 Name	CS1000_Mall	CS1000_ Hospital	CS1000_ College	CS1000_High School
SecurityAdminis-trator (built-in)	• UnRestrict-edOam-Access • SecAdmin • Account Admin	• UnRestrict-edOam-Access • SecAdmin • Account Admin	• UnRestrictedOamAccess • SecAdmin • Account Admin	• UnRestrictedOamAccess • SecAdmin • Account Admin
Patcher	• OamUser • Pdt1Access	• OamUser • Pdt1Access	• OamUser • Pdt1Access	• OamUser • Pdt1Access
E911	• Permission_E911	• Permission_E911	• Permission_E911	• Permission_E911
AnytownAdmin	• UnRestrict-edOam-Access	• UnRestrict-edOam-Access		
AnyCityAdmin			• UnRestrictedOamAccess	• UnRestrictedOamAccess

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.

The following table shows the administrator role assignments for ABC company.

Table 21
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 the previous table, 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 CS 1000 systems.
- Jin performs the maintenance work of CS 1000 systems of Anycity.

Appendix Red Hat passthrough end user license agreement

ATTENTION
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

H

I

L

M

P

R

S

T

U

V

W

Nortel Communication Server 1000

Enterprise Common Manager Fundamentals

Release: Release 5.5
Publication: NN43001-116
Document revision: 02.12
Document release date: 26 November 2008

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

www.nortel.com
Sourced in Canada

NORTEL