Nortel Communication Server 1000

Unified Communications Management Common Services Fundamentals

Release: 7.0
Document Revision: 04.01

www.nortel.com

NN43001-116

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-116
Document release date: 4 June 2010

Contents

New in this Release

The following sections detail what is new in the *Unified Communications Management Fundamentals* (NN43001-116) for Nortel Communication Server 1000 Release 7.0.

Navigation

Features

See the following sections for information about feature changes:

Navigation

Search and filter

A search and filter capability is introduced in Release 7.0. The search operation is performed on the data in persistent storage and the matching result and search criteria are stored in memory for future use. The filter operation is performed to get matching results of a search criteria from memory. You can search and filter from the Elements page, the Certificate Management page, and the Secure FTP Token Management page.

Other

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

Revision History

June 2010 Standard 04.01. This document is up-issued for Nortel Communication Server Release 7.0.

August 2009 Standard 03.07. This document is up-issued for Nortel Communication Server Release 6.0. More clarity was added to the procedures about changing the FQDN of a member server.

July 2009 Standard 03.06. This document is up-issued for Nortel Communication Server Release 6.0.

July 2009 Standard 03.05. This document is up-issued for Nortel Communication Server Release 6.0.

June 2009 Standard 03.04. This document is up-issued for Nortel Communication Server Release 6.0.

June 2009 Standard 03.03. This document is up-issued for Nortel Communication Server Release 6.0.

May 2009 Standard 03.02. This document is up-issued for Nortel Communication Server Release 6.0.

May 2009 Standard 03.01. This document is up-issued for Nortel Communication Server Release 6.0.

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

This document contains information about the components, features, and benefits of the Unified Communications Management (UCM) Common Services. It describes UCM security management, including the various user account and identity configuration options and security policies for password thresholds. The document describes authorizations and permissions for built-in and custom role permission assignments that provide access control to the Common Services.

This document also provides information for the following tasks:

- how to review and configure local account password policies
- how to manage and configure elements within UCM
- how to manage and configure users, roles, and permissions within UCM
- 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 UCM

Navigation

- "UCM overview" (page 15)
- "Security Services overview" (page 43)
- "Security server configuration" (page 57)
- "Logon and logoff options in UCM" (page 81)
- "UCM Network configuration" (page 89)
- "UCM User Services configuration" (page 113)
- "UCM Security configuration" (page 131)
- "UCM Tools configuration" (page 159)

UCM overview

This chapter provides an overview of Unified Communications Management (UCM) Common Services and the required components.

Navigation

Introduction

The UCM solution provides an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You have access to all network system management elements under the Unified Communications Management solution. You need to sign in only once to access the elements. A single sign-on eliminates the need for you to reauthenticate when a system management application starts.

UCM Security Services simplifies security control for managed elements and system management applications. UCM Security services manage secure access to Web applications and provide authentication and authorization with a single unified Common Service. UCM secures the delivery of essential identity and application information.

With UCM Common Services, 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 UCM Common Services, 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.

UCM Deployment Manager provides two methods for software deployment:

- centralized software deployment (recommended)
- local software deployment

UCM Common Services supports Microsoft Internet Explorer 6.0, 7.0, and 8.0. Other versions and browsers are not tested or supported.

Linux Platform Base and Applications can run on the following hardware platforms:

- CP PM card
- CP DC card
- CP MG card
- COTS Servers
  - IBM x306m
  - HP DL320 G4
  - IBM x3350
  - Dell R300

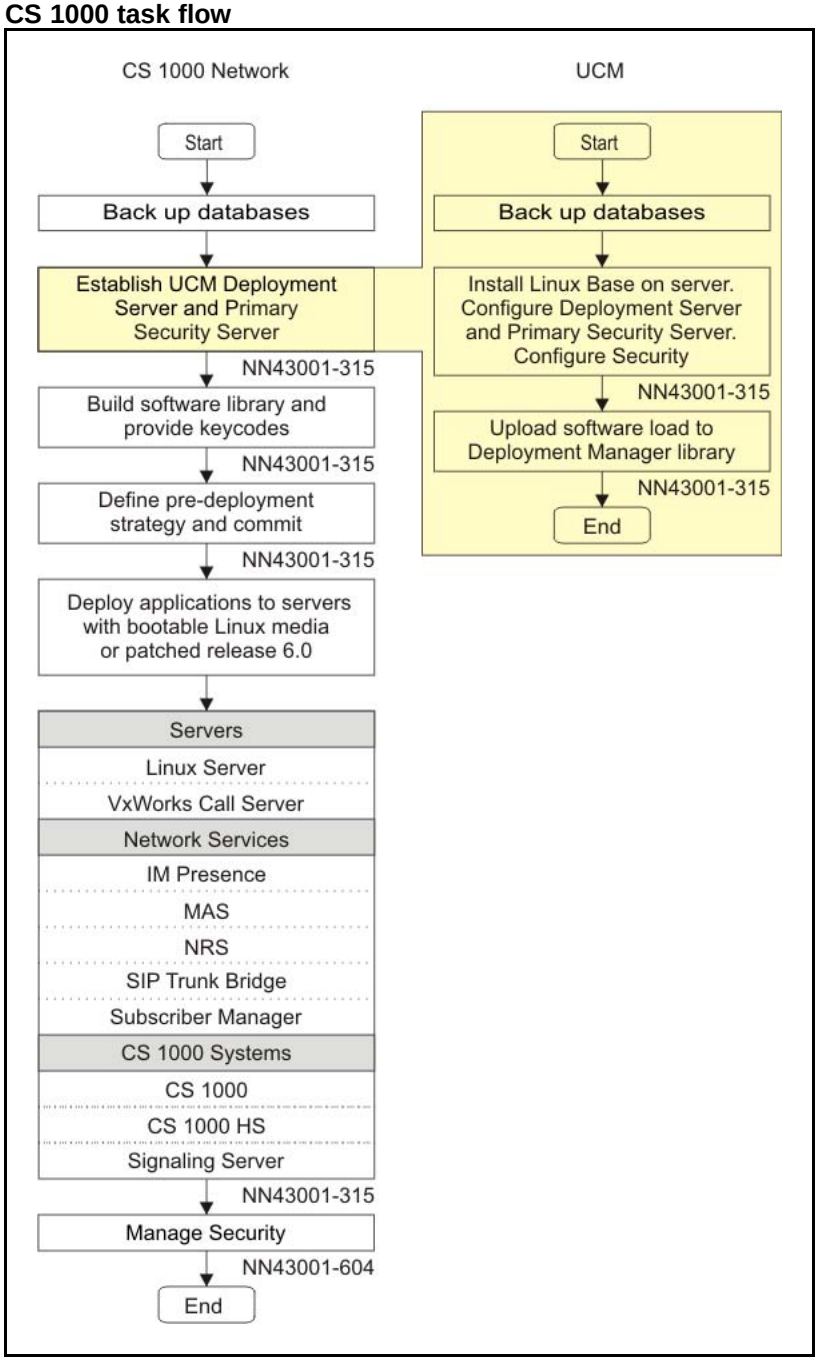
ATTENTION
To connect a terminal to the IBM X3350, you require a 9-pin female to 9-pin female null modem cable, part number NTRX26NPE6.

You require only one primary security server for each secured domain. A network supports only one backup security server. Replication is unidirectional from the primary to the backup. You can perform all administrative changes, for example, security configuration and identity management, on the primary security server.

Communication Server 1000 task flow

This section provides a high-level task flow for the installation or upgrade of a Communication Server 1000 system. The task flow indicates a recommended sequence of events to perform when you configure a system and provides the technical document number that contains the detailed procedures required for the task.

Figure 1
CS 1000 task flow



For more information, see the following technical documents.

- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000E Software Upgrades* (NN43041-458)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *SIP Line Fundamentals* (NN43001-508)
- *Security Management Fundamentals* (NN43001-604)

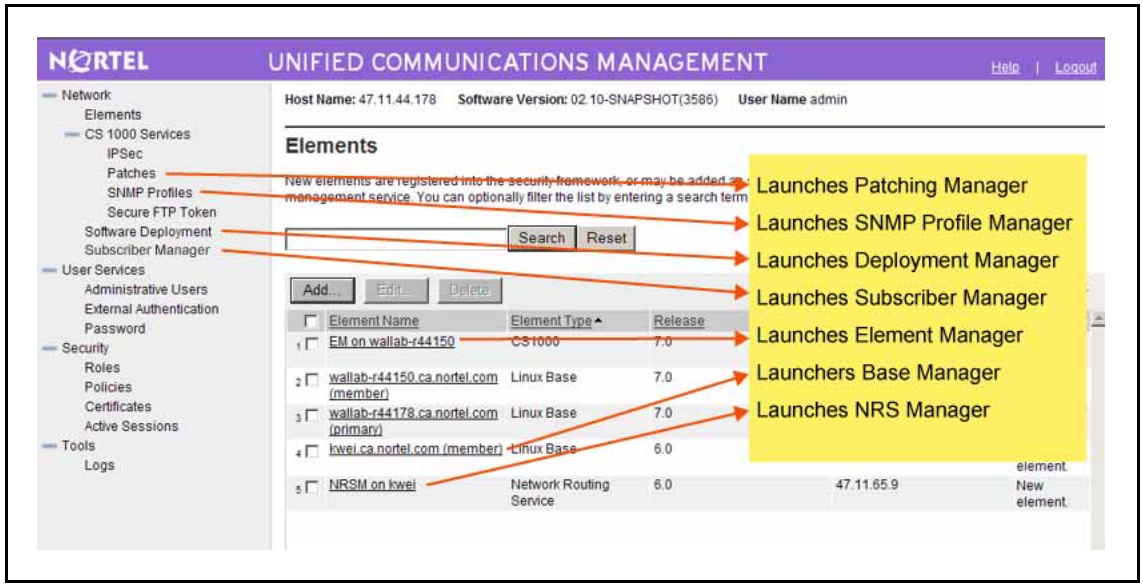
UCM navigation tree

The UCM navigation tree is on the left side of the Web page. The root level branches are as follows:

- Network: Network-level objects, network navigation, and device management
- User Services: User-related objects and identity management
- Security: UCM Security Services objects and security policy management
- Tools: Logging services

The following figure depicts the UCM main navigation page.

Figure 2
UCM main navigation page



UCM basics

Two methods are available to use the UCM Common Services interface: table view and tree view.

- The table view is the default view. From the table view, you can add, edit, or delete elements. For more information, see “Table view” (page 20) .
- The tree view is a hierarchical view. From the tree view, you can create groups of elements according to your business needs. For example, an administrator can create a group in the tree for elements that are part of a specific CS 1000 node. You can nest groups. For more information about using the tree view, see “Tree view ” (page 20).

Use the following icons on the UCM main navigation page to change your view. To update the list, click the refresh icon.

Figure 3
Element icons

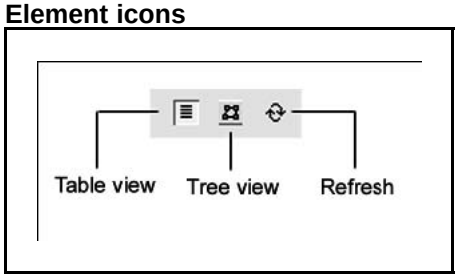


Table view

Table view is the default view on the Elements page. You see a list of UCM Common Services elements that are based on your role permissions. A network administrator can see all elements. From the table view, you can add, edit, or delete elements.

Secured elements in Security Services may be subject to authentication because single sign-on is not available for elements outside UCM Security Services. You can search and filter elements from the Elements page. Search for a managed element by Element Name, Element Type, Release, or Address.

Tree view

The Network group is the root level of the tree view. To navigate, click an element name and the Web browser is redirected to the management application of that element. If the element is a secured element in Security Services, no sign-on is required. If the element is a third-party element (such as a Hyperlink element), the administrator is subject to administrator authentication, as single sign-on is not available. In some instances, groups appear as links in the tree, and this indicates that an element is associated with the group. For example, a group representing a node can be associated with the node master element. Click the group name to navigate to the associated element. When the tree appears in navigation mode, only the elements that the administrator is authorized to access appear. The tree expands to the second level by default.

The System Groups contains two member groups: All Elements and System Types. The All Elements group contains all the elements visible in the list view sorted alphabetically by element name. The System Types group contains groups of elements by system type, such as CS 1000 or Hyperlink. Elements in each folder are sorted alphabetically by element name. Click an element in a system group to navigate to the management application running on that element.

Central launch point and common User Interface

The UCM security domain provides a central launch point for installed managed elements and hyperlinks. You can access a managed element when you log on to UCM Common Services or through a direct Web link.

On the Elements Web page, you can access an element by performing one of the following tasks:

- Click an element item

The selected element starts in the current browser window and replaces the UCM Common Services or element interface.

- Right-click the element to open the element in a new browser window.
- Select an element from the Favorites list in the browser window.

  The selected element starts in the current window and replaces the UCM Common Services or element interface.

  To add an element to your Favorites list, right-click the element and select Add to Favorites.

UCM Common Services is a common User Interface that remains consistent between other element applications. UCM Common Services displays the items, specific to the selected element, in the left navigation pane. For example, if a user selects NRS Manager from the element list, the NRS Manager replaces the UCM Common Services interface in the browser window and the NRS Manager navigation items appear in the left navigation pane.

Click Common Manager from the navigation pane to return to UCM Common Services.

Button bar

The most frequently used commands are available in the top right-pane of the Edit Navigation tree. Frequently used commands are Add Group, Remove, Edit, and Undo. These commands are also available from the shortcut menu when you right-click an element or group.

ATTENTION
Buttons appear dimmed if you do not select the appropriate number of elements for a command.

Undo feature

Use the Undo button in the button bar to cancel the last modification to the tree. You can undo up to 10 changes. If you saved the changes to the Edit Navigation tree, you cannot undo the changes.

Cut, Copy, and Paste commands

You can use cut, copy, and paste to move items in the tree or to copy groups.

- For a single item, right-click the item and select Copy from the shortcut menu.
- For multiple items, hold the **Ctrl** key and left-click the items to copy or move. Right-click on the selection and select Copy from the shortcut menu.
- For a range of items, left-click the first and last items. All the elements between and including the first and last item are selected. Right-click the selection and choose Copy from the shortcut menu.

Paste the selected items by right-clicking the destination group and choosing Paste from the shortcut menu.

The items in the copy buffer are added to the bottom of the destination group.

ATTENTION

The target of a paste operation must be a group.

You can paste items in the copy buffer multiple times until the copy buffer is over written by another copy operation.

Items that are cut but not pasted into the tree are removed from the tree.

Network

The Network section contains the following items:

- “Elements” (page 89)
- “CS 1000 Services” (page 110)
- Subscriber Manager

Elements

The Elements page is the default Web page that opens when UCM Common Services starts. 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. You can also access base manager by clicking on an element.

Users can add, edit, or delete elements within Security Services.

The following is a list of the supported element types:

- Linux base
- CS 1000
- Network Routing Service Manager (NRSM)
- Media Gateway Controller (MGC)
- MC32
- Hyperlink
- CallPilot (Available only when Subscriber Manager is deployed.)

  When you click on the CallPilot element, you are redirected to the CallPilot logon page that was configured for the selected element. Use your CallPilot logon credentials to log on.

ATTENTION
Users see only the elements that are enabled based on the assigned role permissions.

CS 1000 Services

This section contains the following items:

IPsec

IP security (IPsec) is centrally managed from the UCM Primary Security server using the IPsec for Intra System Signaling Security (ISSS) management interface. ISSS employs IPsec to provide security services, including confidentiality, authentication, and anti-replay, to application layer protocols.

From the ISSS interface on the Primary UCM server, you can administer several aspects of IP security, such as configuring a domain-wide security policy, adding and removing IPsec targets, enabling or disabling IPsec for network elements, and scheduling IPsec synchronization and activation.

Changes to the security policy are securely distributed to the network elements by the UCM transfer mechanism and activated according to a schedule defined by the administrator. Automatically scheduled distribution and activation allows changes to IPsec configurations without individually reconfiguring each element in the UCM security domain.

The ISSS management interface lists all Communication Server 1000 and Communication Server 1000 HS systems available on the UCM domain. ISSS can be enabled only on those UCM targets which belong to a CS 1000 system or CS 1000 HS system. ISSS parameters (PSK & level) are specified as a Security policy that can be applied to one or more Communication Server 1000 systems or a Communication Server 1000 High Scalability (HS) systems. ISSS operations like Synchronization and Activation can be performed on one or more CS 1000 systems simultaneously.

For procedures relating to ISSS, see *Nortel Security Management Fundamentals* (NN43001-604).

Patches

Use Patching Manager by logging on to UCM from the primary security server to remotely deploy patches from a central location to other Linux servers on the same security domain. From the CS 1000 server, click Patches. A central patching library is maintained and patches can be uploaded and centrally deployed on all Linux elements in the security domain.

You can install patches locally. Local Patching is accessible from the Base Manager of each Linux Element. Access Patching Manager by logging on to the primary security server and clicking an element or by logging on locally to the element.

Accounts must have Patch Administrator permissions assigned for access to Patching Manager. Local logon users have full permissions to use the local Patching Manager. For more information about Patching Manager, see *Patching Fundamentals* (NN43001-407).

SNMP Profiles

Use the Simple Network Management Protocol (SNMP) Profile Manager to perform configuration at the network level for CS 1000 and stand-alone UCM elements such as a stand-alone primary security server and stand-alone NRS. You can configure using the following:

- SNMP Profile: Configure SNMP profiles in UCM such as adding or deleting.
- SNMP Distribution: Assign and send SNMP profiles to Elements configured in UCM.

To send SNMP traps, you must configure SNMP parameters such as the SNMP trap destination. You can centrally configure the SNMP parameters including the SNMP trap destination in profiles by using SNMP Profile Manager. SNMP profiles are then assigned and propagated to all devices in the UCM security domain. You must configure SNMP for the Linux

element; otherwise, no information is available about where to send SNMP traps. For more information about configuring SNMP Profiles, see *Communication Server 1000 Fault Management — SNMP* (NN43001-719).

Secure FTP token

From the CS 1000 Services, click Secure FTP Token. The Secure FTP Token Management page appears on which you can view the date of the most recent generated token, refresh the status of the current token, and regenerate a new token for distribution throughout the network.You can search and filter for secure FTP token endpoints by typing in the endpoint address or token transfer status from the Secure FTP Token Management page. For more information about Secure FTP Token, see *Security Management Fundamentals* (NN43001-604).

Software Deployment

Use Deployment Manager on the Primary security server for an end-to-end installation and configuration of Linux Base and applications. Deployment Manager provides a simplified and unified solution that enables network installation of Linux Base on target servers. The Primary security server is the Deployment Server.

On the UCM navigation pane click Network, Software Deployment. The Deployment Manager Web page appears on which you can select the following:

- Deployment View
- Software Loads
- Backups
- 6.0 Deployment Targets

You can deploy software locally before the server joins the security domain; however, Nortel recommends that you use the central deployment method.

For more information about Software Deployment, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

User Services

In the User Services branch of the UCM navigation tree, you can select the following items:

- Administrative Users: You can view administrative users, add a new administrative user, or disable or delete an existing administrative user.
- External Authentication: The External Identity Repositories Web page contains a summary page for authentication scheme and authentication servers. In the Authentication Servers page you can

configure an LDAP server, RADIUS (Remote Authentication Dial-in User Service) server, or a Kerberos server. For more information about configuring these servers, see “Provision the authentication servers” (page 123).

- Password: View the status for a password or to change the password.

Security

In the Security branch of the UCM navigation tree, you can select the following items:

- Roles: 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.
- Policies: Configure the authentication scheme and authentication servers, establish password policies, and edit security settings.
- Certificates: Configure the information for certificate configuration status.
- Active Sessions: Display all users who are currently logged on and the session time for each user.

For more information about Security configuration, see “Navigation” (page 131).

Tools

In the Tools branch of the UCM navigation tree, you can select the following items:

- “Logs” (page 26)
- Data

Logs

In the Tools branch of the UCM navigation tree, click Logs. The Logs Web page appears.

From the central UCM primary security server, use the log viewer tool to view Security and Operation, Administration, and Maintenance (OAM)-related audit logs.

Log on as network administrator to perform the following functions:

- Filter the log based on the query string and event types.
- View the log for a specific date.

- Configure the remote SYSLOG server to forward audit logs in real time to the third-party Operational Support System (OSS) SYSLOG server for monitoring and analyzing.
- Export the log as a comma-separated value (CSV) file.

ATTENTION
You must log on as a network administrator to view the Logs link.

No restrictions exist to the number of users that can simultaneously access the Log Viewer tool when they log on with the network administrator role. Log files must be less than 5 megabytes (MB) to view using the Log Viewer tool. If the log file size exceeds 5 MB, a link is available to export and download the file.

Log storage Operation, Administration, and Maintenance (OAM) and application logs are stored on the Linux server where they are generated. For optimal access control and to maintain an audit trail of all system administrator activities and security-related events, the OAM logs from the backup and member servers are forwarded to the UCM primary security server as the central storage location. OAM logs are provided for the CS 1000 management applications running on a Linux platform to record security, operational, configuration, and maintenance events. Application logs are stored locally on a Linux server and are not forwarded to the primary security server for consolidation.

The oam.log and security.log files are created daily on the primary security server with the date appended to the log file name. The logs are stored in /var/log/nortel/OAM. You must restart the syslog service at the CLI level when you manually modify the syslog files. To restart the syslog service, log on as a root user and run the command **`/sbin/service rsyslog restart`**.

During the Linux base installation, 10 percent of the total hard disk space is allocated for the storage partition and cannot be changed. Storage for all log files of Nortel applications can be stored in /var/log/nortel. You can access these log files by logging on as a root user at the CLI level. The Linux base alarm script monitors the partitions. If storage capacity is reached, a Linux console message appears.

Use the Log Viewer Tool to view the application and OAM logs. You can display the log for the last 30 days, sort by field, or filter and export the log as a comma-separated value (CSV) file.

ATTENTION
The log files are stored on the primary security server and have a 30-day rotation.

Log configuration

The following table shows the logs files stored in the /var/log/nortel/OAM folder of the UCM primary security server.

Table 1
UCM primary security server log files

Log file type	Description
OAM logs are stored in two files based on the type of logging event:	
Audit logs: oam.log	Storage location of all OAM administration events that occur from the CS 1000 management applications running on a Linux platform: • Operational events—captures the query for status and enabling or disabling resources. • Configuration events—captures all the feature or functional provisioning and modifications. • Maintenance events—captures all the upgrades, backups, restores and patching.
Security logs: security.log	Storage location of all security related events: • security policy changes • Linux CLI messages—captures logon and logoff attempts. • logon success and failures • certificate changes • user account creation and illegal (failed) login events • Any OAM security event where network administrator privilege (or flag) is enabled or required.
Application logs are generated using the Syslog framework at a Linux operating system level. View Application logs stored on a local system by using the Log Viewer tool from the base manager.	
Application logs	These applications include the following: • LTPS • SIP Line Gateway • SIP Signaling Gateway • NRS Routing bundle (NCS, H323, and SIP Redirect Server) • Management bundle • Linux Base log • CP PM Co-resident Signaling Server • Any other Nortel-specific application log

Forwarding logs to third-party OSS The consolidated OAM audit logs from the primary security server can be forwarded in real time to external third-party Operation Support System (OSS) Syslog servers for monitoring and analyzing. You must configure the third-party OSS syslog server

before audit log forwarding can occur. The following is the list of values assigned to each severity level.

- Emergency: 0
- Alert: 1
- Critical: 2
- Error: 3
- Warning: 4
- Notice: 5
- Information: 6
- Debug: 7

Severity is listed in order of lowest priority. All messages with the selected priority and the priorities below it are forwarded, for example, if you select Alert, this forwards Alert and Emergency messages.

For more information about configuring, see "Configuring or editing the configuration of logs for forwarding to third-party OSS" (page 161).

ATTENTION
Only OAM logs from the primary server can be configured for forwarding. Application logs based on syslog format cannot be forwarded using this feature. Once the configuration is saved, the forwarding of the OAM audit logs occurs.

Archived files The archived files for both oam.log and security.log are in a compressed format. The naming convention for the archived files is xxx.log-YYYYMMDD.gz.

Applications and services

The following table identifies the applications deployable within the UCM Common Services.

Table 2
UCM Applications

Services and applications	Description and document reference
UCM Patching Manager	The Patching Manager centrally deploys patches from the primary security server to other Linux servers in the same security domain. For more information, see "Patches" (page 24) and *Patching Fundamentals* (NN43001-407).

Services and applications	Description and document reference
UCM Deployment Manager	The Deployment Manager on the Primary security server (Deployment Server) provides an end-to-end installation and configuration of Linux base and applications on a Server. Deployment Manager also provides backup services of Linux elements. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
IPsec Manager	The IPsec Manager centrally configures security services, including confidentiality, authentication, and anti-replay, to application layer protocols from the primary security server. It configured IPsec settings for all elements in the security domain. For more information, see *Security Management Fundamentals* (NN43001-604).
CS 1000 Element Manager	See *Element Manager System Reference — Administration* (NN43001-632).
Network Routing Service Manager	The NRS Manager runs on the same element as NRS. NRS Manager centrally configures, provisions, and maintains the NRS from the primary security server to other Linux servers in the same security domain. For more information, see *Network Routing Service Fundamentals* (NN43001-130).
Base Manager	The Base Manager, a Web-based interface, is used for low level configuration of all Linux elements. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
Subscriber Manager	The Subscriber Manager centrally manages subscribers and subscriber accounts from the primary security server. For more information, see *Subscriber Manager Fundamentals* (NN43001-120).
SNMP Profile Manager	The SNMP Profile Manager centrally configures SNMP parameters for all elements from the primary security server to other Linux servers in the same security domain. For more information, see *Communication Server 1000 Fault Management — SNMP* (NN43001-719).
Secure FTP Token	The Secure FTP Token on the UCM Backup security server refreshes the status of the current token or regenerates a new token for distribution throughout the network. For more information, see *Security Management Fundamentals* (NN43001-604).

The following table identifies the services that are intrinsic to the UCM Common Services management framework.

Table 3
Services

Services	Description and document reference
UCM Security Service	Security Service is the primary interface for system-wide security configuration and administration and provides centralized authentication for users, systems, and devices by operating as a RADIUS server, providing authentication for RADIUS clients based on defined roles and policies. For more information, see "Security Services overview" (page 43) and *Security Management Fundamentals* (NN43001-604).
UCM Web Service	Web Service provides a common navigation hierarchy for installed management applications. With Web Services, you can develop new applications and customize scripts. For more information, see *Web Services API Applications* (NN43001-640).
UCM Logging Service	The Logging Service securely maintains a central audit trail of all system administrator Operation, Administration, and Maintenance (OAM) activities and security-related events. From the primary security server, you can use the log viewer tool to view Security and OAM-related audit logs. For more information, see *System Management Reference* (NN43001-600).

UCM client capacity

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

Table 4
UCM client capacity

UCM, element, and administrator thresholds	Maximum capacity
The maximum number of elements supported in one UCM	1000
The maximum total number of elements supported in multiple UCMs	1000
The maximum number of UCMs supported within a network	6
The maximum number of Linux members elements	200
The maximum number of Vxworks Elements (MC/MGC/CS)	200
The maximum number of concurrent active administrators supported within an UCM network	40
The maximum number of groups supported in UCM	50
The maximum number of administrators configured on one UCM	500

UCM, element, and administrator thresholds	Maximum capacity
The maximum number of administrators connected simultaneously on one UCM	10 **ATTENTION** Although 10 administrators can connect 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 UCMs	5

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

You can increase the number of elements by adding supplementary UCM servers. Regardless of the number of UCM servers installed, all elements within the same security domain appear in each UCM navigation tree.

Benefits and features

UCM Common Services 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 User Interface look and feel across all supported management facilities
- Web service interface where third-party developers can create applications to access UCM
- registry of the managed elements that start the management applications
- security that provides Authentication, Authorization, and Auditing (AAA) for plug-in Web applications (elements) that reside within UCM Common Services
- central 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 Based Access Control (RBAC) and Instance Level Access Control (ILAC)
- central point to manage users, passwords, and system access

Central authentication

The UCM Common Services provides a central GUI-based interface for individual account administration for the Nortel Communication Server 1000 network. This authentication feature implements a RADIUS client that authenticates with the external UCM security server for all VxWorks software platforms the current Communication Server 1000 supports.

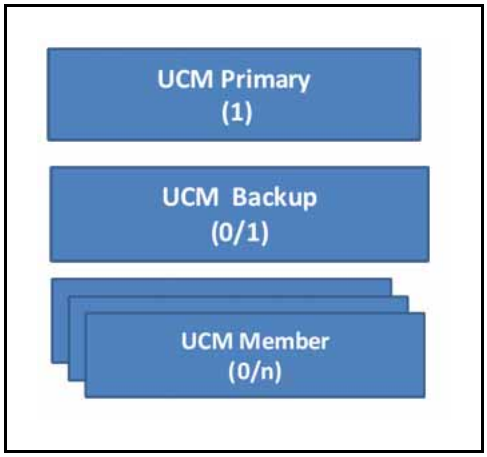
When a user attempts to gain access to any VxWorks system in the Communication Server 1000 network, they are prompted for a user name and password. The user name and password are encrypted and transferred to the centralized UCM security server by the RADIUS verification protocol. The UCM operates as a RADIUS server providing authentication for RADIUS clients. If the user name is defined in the UCM database, the user access is granted to the system with the privileges assigned to them as defined in the UCM database. Each VxWorks system and UCM database has a series of pre defined roles and groups.

Security domain

A UCM security domain is defined by the UCM primary security server. The UCM security domain comprises the UCM primary security server, the UCM backup security server, and associated member servers that contain UCM Common Services and management applications. Each primary and backup security server must co-reside with an instance of the LDAP server. Replication is unidirectional, from the LDAP primary to the backup. 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. The security domain can have 0 or 1 backup servers and additional servers are member servers, as shown in the following figure.

Figure 4
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 servers in the security domain use the primary security server for authentication, authorization, and audit log storage. The **joinSecDomain** command, used to join the UCM security domain, uses the SSH client to communicate with the UCM primary security server but does not provide shell-level access. A VxWorks device joins UCM security domain by using the **joinSecDomain** command and a mutually trusted SSH tunnel is established with the UCM primary security server. VxWorks devices also send information such as a RADIUS secret over the channel to UCM which provides a unique secret with UCM for securing RADIUS communication. Shell level access to users is not provided. Support for Unsecured remote access methods such as rlogin and Telnet is available on the CS 1000 but you can disable them. For more information, see *Security Management Fundamentals* (NN43001-604).

When replication initializes between the backup security server and the primary security server, the backup security server is in 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 and authorization.

A management system can have one or more UCM servers 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 UCM Common Services. UCM Common Services provides the features and capabilities for all installed elements.

When a user logs on to UCM Common Services, the Elements Web page displays a list of installed elements. Reauthentication to access a different element within UCM is not necessary.

Certificate management

UCM uses certificate management: the X.509 certificate for Web Secure Sockets Layer (SSL) for secure communication between a Web browser and a Web server. The following built-in certificates types are available:

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

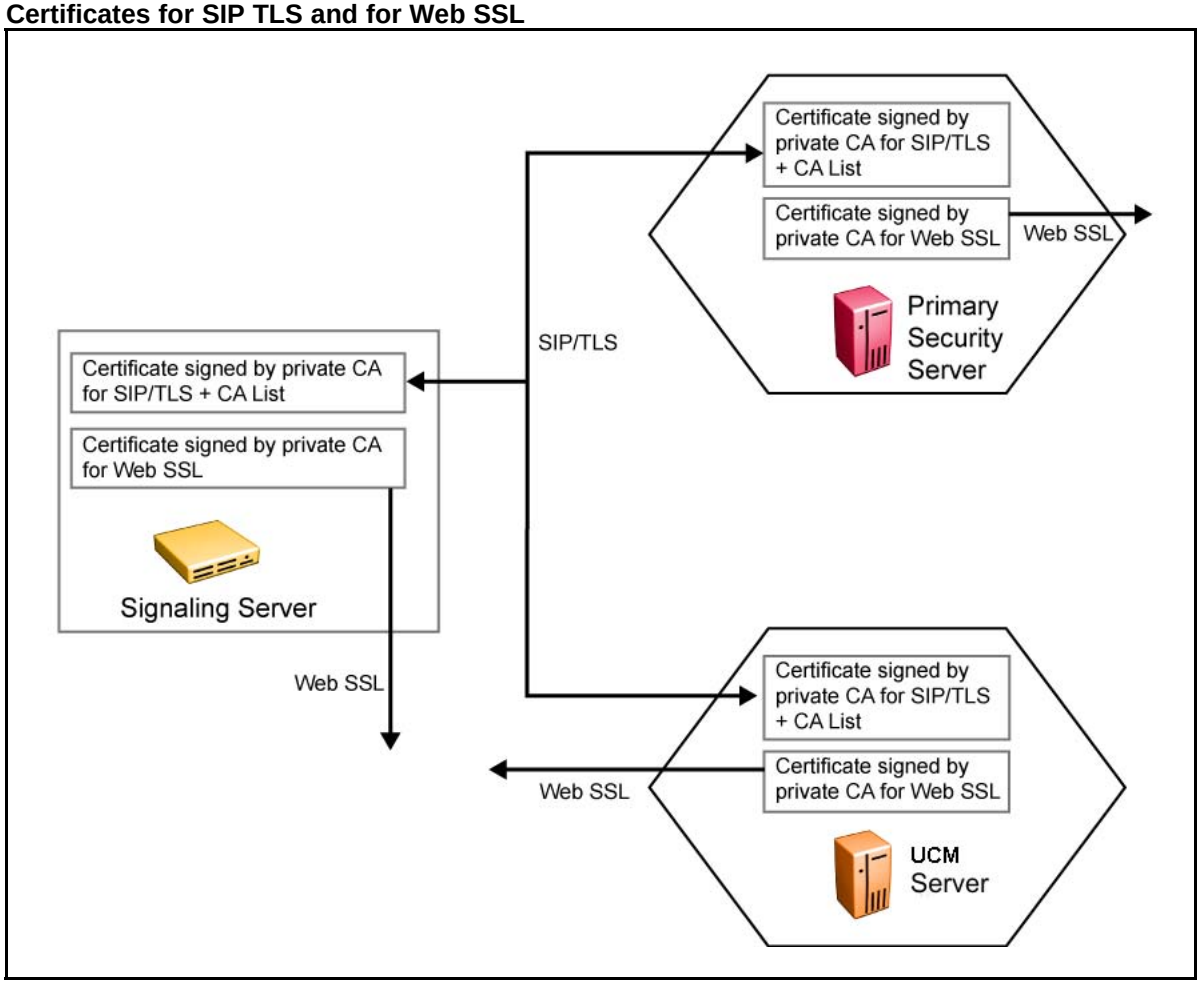
An Administrator can revoke certificates that were previously issued.

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

ATTENTION
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, you can install a certificate signed by the private CA on the server for Web SSL, as shown in Figure 5 "Certificates for SIP TLS and for Web SSL" (page 36).

Figure 5
Certificates for SIP TLS and for Web SSL



ATTENTION
You must configure certificate management through the primary security server Web interface. You cannot manage certificates in Web interfaces on other Linux servers.

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 UCM is installed when you install the application. The network administrator must configure the Web SSL certificate through the Certificates link of UCM on the primary security server.

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

Server types

This section describes the UCM security server roles. For more information about the configuration options, see “Security server configuration” (page 57).

Primary security server

Only one primary security server is required on a network. This server stores all administrator identities, authorization data, and security configuration data. The server contacts and queries all authentication, authorization, and logging. Administrators use the primary security server for navigation to UCM Common Services, network navigation, and the launch pad for network applications such as Subscriber Manager. A primary and backup security server can be demoted to a member server. For more information, see “Demoting a primary and backup server” (page 77).

The primary security server provides the following roles:

- Private certificate authority: only the primary security server can issue certificates for new member servers. The certificate management console access is only from the primary security server.
- Write access to all security-related data: configuration of all options in UCM Common Services can occur only on the primary server.

Backup security server

The role of the backup server is to manage authentication and authorization requests when the primary server cannot be contacted. The backup server is optional. Any server can be designated the backup security server, and only one backup security server can be on a network. You can start the backup server by accessing http://<FQDN of backup>. If you log on to the primary server and it becomes unavailable, you must log on to the backup server. The following figure shows the items that are available from the navigation pane. Subscriber Manager also appears in the navigation pane if you deploy it.

Figure 6
Backup server navigation pane

The backup security server provides the following roles when the primary server is unavailable:

- All authentication and authorization requests are managed.
- All certificates continue to function.
- Audit logs are recorded when the backup server handles authentication. No log synchronization occurs between the primary and backup. Nortel recommends that you manually transfer the OAM log files from the local servers to the primary security server and append them to the OAM file for that day.

ATTENTION
You can use the backup security server to configure changes such as adding new administrators . The UCM Web pages and network navigation are available for viewing but the Certificate Management pages are not available for viewing or changing. The backup security server cannot be promoted to a primary security server . The backup server always maintains real-time synchronization with the primary server. A backup security repository is part of the backup server installation. This repository is read-only.

Member server

The member server is part of a secured network and is not a primary or backup security server. A member sends all security requests to the primary security server. No access is available to UCM Common Services and LDAP server is not running on it. For emergency situations, you can use a local logon page.

When an administrator types the URL of the member server, the member first verifies that the primary server is running. If the primary is running, then the user is forwarded to the primary server. If the primary is down then the user is forwarded to the backup. If the backup is also down, then the user goes to the local logon page of the member server.

If you try to access an application running on a member server, the member server attempts to use the first security server that responds, for example, a primary or backup server. The first primary or backup server to respond is the one closest to the member server. This approach is intended to load balance the security servers. Therefore, for a RADIUS server on the security domain, the radius server must have records for both the primary and backup security servers with the same shared secret.

No session failover occurs on the member server. If an administrator is logged on to the primary server and it becomes unavailable, the administrator must log on to the backup server.

ATTENTION
You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.

Domain Name System

During the Linux base installation, you are prompted to configure the Domain Name System (DNS) server IP address. Users can also manually configure the DNS after installing the Linux base. 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).

Disaster Recovery

A file backup and restore option supports the disaster recovery mechanism for the Linux Base and Nortel applications including UCM. For information about prerequisites and procedures for Nortel Linux system disaster recovery on a COTS or CP PM server, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

High Availability configuration

High Availability (HA) provides continuous availability and reliability in case the active server fails or abnormally terminates. High availability is achieved by replicating the security repository, configuring a backup server, and replicating the admin users and policies data for redundancy.

In normal operation, an agent is installed on a member server. The agent talks to the security services on the primary security server. When the member server registers with the primary server, the member server receives a list of backup security servers.

The private Certificate Authority (CA) runs only on the primary security server. The CA is not a point of failure as it is not required to be online during normal operation. The CA is required only to sign Certificate Signing Requests (CSR). When the primary security server is down, certificates between member servers remain valid and trusted because they each maintain a trusted CA list.

ATTENTION

If the primary server must be rebuilt due to new hardware, the IP address and the Fully Qualified Domain Name (FQDN) of the new hardware must be the same as what was previously used.

- The primary security server hosts the private CA that signs a Certificate Signing Request (CSR) from other servers. If the IP or FQDN does not stay the same, then future CSRs signed by the new primary security server cause trust problems with older certificates on other servers.
- The agents on member servers have the FQDN of the primary security server. If the IP or FQDN cannot be reused and rebuilding the admin users, roles, and policies does not occur, then new CSRs must be issued and signed by the new CA and all member servers and backups must be manually updated with the location of the primary security server. Server types are not interchangeable. For example, member servers cannot change to a primary or backup security server.

The following table shows the HA failover scenarios for the primary and backup security servers and member server.

Table 5
Failover scenarios

Primary security server	Backup security server	Member server	Failover scenario
offline	online	online	The member server checks the availability of the primary and backup security server. If the primary fails to reply, the member server switches to the backup security server. Failover can be triggered by failure of the security services, security repository, the network, or any other cause of the member failing to get a heartbeat. Updates to users and policy changes are not allowed on the backup security server. Updates to operational information such as time of last logon and number of logon attempts continues, but changes to this data revert to the previous values when the primary security server is restored.

<table>
<tr><th>Primary security server</th><th>Backup security server</th><th>Member server</th><th>Failover scenario</th></tr>
<tr><td></td><td></td><td></td><td>After the primary security server becomes available and the member server status is detected, the member server then switches back to the primary security server without administrator intervention. No manual process triggers failover or fallback.

The audit trail logs are maintained independently on all security and member servers when the primary is down. When the primary server becomes available, the logs must be manually sent to the primary security server and appended to the OAM file for that day.

Manual Replication can be performed from the backup security server from Tools, logs. After the administrator clicks Manual Replication, the backup data store copies everything from the primary data store. The backup data store synchronizes with the primary data store. Manual replication is performed only for disaster recovery purposes.</td></tr>
<tr><td>offline
continued</td><td>online
continued</td><td>online
continued</td><td>ATTENTION
Nortel strongly recommends that you do not run in the failover state for extended periods of time as logs can be lost on the backup and member servers if you exceed the storage limits.

Admin user and policy configuration changes are not allowed when the primary security server is not available.

 
CAUTION
Changes to the backup server are not supported if the primary server is operational but is unreachable due to a network problem. Do not make changes to the backup server under these conditions.</td></tr>
</table>

Primary security server	Backup security server	Member server	Failover scenario
offline	offline	online	When a member server switches to the backup server and the backup server fails or when the member cannot reach either the primary or backup server, the member is taken to the local logon page of the member server. The administrator can log on and perform emergency configuration in the local logon page.
online	offline	online	The reload data tool cannot be run on a primary server when the backup server is offline. Everything works as usual; however, if the Primary server goes offline, the system is not accessible because the backup server is not working.

Security Services overview

The Unified Communications Management (UCM) Security services enables element and service management applications to access a common application security infrastructure. Security manages secure access to Web applications and provides security for Web interfaces and Web utilities.

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

Access to various security features that enable administrators to configure user and security rights within the application server are provided. Network administrators can create custom roles or use the built-in roles. Permissions can map to roles for each user. For more information, see “Built-in roles” (page 50) and “Custom roles” (page 54).

ATTENTION
The pages are view only, unless you permission to perform operations such as editing and deleting.

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user.

Navigation

- “Authentication” (page 43)
- “Security policies” (page 46)
- “Access control policies” (page 48)

Authentication

Authentication verifies the user logon identity. The user authentication is based on an assigned password.

Identity management

With identity management, network 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 various user accounts for different managed elements.

The UCM Security Services supports the following account types:

- local account
- built-in account
- external account

Accounts

Use the following information for UCM Security.

Local account

The UCM Security maintains the data entry and password for a local user account; which is stored in persistent storage.

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

Table 6
Types of status for local user accounts

Status Type	Description
Enabled	An account with enabled status can log on to UCM according to the roles and permissions assigned.
Disabled	An account with disabled status cannot log on to UCM.

Built-in account

UCM Security has one built-in account that is used by network administrators to log on to UCM Common Services after installation. The built-in account is assigned to built-in roles.

The following table describes the supported built-in accounts.

Table 7
Supported built-in accounts

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

Table 7
Supported built-in accounts (cont'd.)

admin	No default password. The admin password is created during configuration.	NetworkAdministrator	Use this account as the default account to log on to the UCM Common Services after a new installation. You use this account to create individual user accounts. See the Attention box below for important information regarding security best practise for the admin account.
nortel	No default password. The nortel password is created during the Linux base installation.	none	Use this account when the administrator password is forgotten, the admin account is locked out, or to access EM when the primary security server is down.

ATTENTION
With the built-in admin account, administrators can add, delete, and edit managed elements. Administrators can control the users who have direct access to specific managed elements. Administrators 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.

Nortel recommends as a security best practise that administrators create new accounts and assign roles to those accounts for access to the managed elements based on your security policy requirements. The admin account should be disabled after these new accounts are created. For more information about role assignment, see Table 10 "Built-in roles" (page 51).

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), Kerberos server, the external administrator account is added to UCM.

Administrators can configure only one RADIUS or LDAP external authentication authority.

An external user has a shadow entry inside the persistent repository of the UCM Security Services. Security Services uses the shadow entry to assign roles to the external user.

ATTENTION
The network 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 by using UCM Common Services.

Central logon

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

Central logon is different from Single Sign-On (SSO). Central logon 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 Communication Server 1000 system, central logon refers to the command line interface (CLI) access for Linux hosts.

Security policies

With the UCM Security, you can configure password and authentication settings.

Password aging policy enforcement

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

- Minimum password age
- password expiration warning
- password expiration

The following table describes what occurs when a user logs on to UCM Common Services when the password aging policy thresholds expire.

Table 8
Password aging policy thresholds

Password threshold	What occurs when a threshold has expired
Minimum password age	You cannot change the password until the minimum password age has been reached. For example, you cannot change the password for three days after the last change was made.
Password expiration warning	You receive a password expiration warning when the password is about to expire and before the password expires.
Password expiration period	You are 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 network administrator. For example, if your password expiration period is configured to 90 days and the expiration warning is 15 days, you start receiving password expiration warnings 15 days prior to the password expiring. After the password expires, you have three opportunities to logon and change the password before the account is disabled. There is no time limit associated with the three logon opportunities. If you do not change the password during the three additional logon opportunities, the account is disabled on the fourth logon attempt and the network administrator must reset the user account password.

WARNING
The password expiration warning message does not appear on the CLI of VxWorks Call Servers. You cannot change the password from a VxWorks server if the password has expired. If the password expires, you see an invalid logon message when attempting to log in to the VxWorks Call Server. At this point, the account is locked and the network administrator must reset the user account password.

The password strength policy enforcement

Passwords must contain a combination of alphanumeric and special characters as defined by the network administrator. The password strength policy enforces the following constraints.

- Passwords must have a total character length between 6 to 25. Default is eight.
- Passwords are not required to have a minimum character type; however, the default is one lower- and upper case character, one numeric character, and one special character, such as an exclamation mark (!). The sum cannot exceed the minimum total length.

After the password strength policy is enabled, the following passwords standards must be met.

- Password must not have a character repeated more than twice consecutively.
- Passwords must not be your User ID, in forward or reverse order.

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

ATTENTION
The password strength policy can be disabled.

Password history policy enforcement

The password history policy verifies that a password is new. The previous blocked passwords can range from 1 to 99. The default is six.

Password lockout policy enforcement

The lockout policy provides a limit for the number of attempts to access UCM Common Services. The user is locked out of UCM Common Services when the specified number of logon attempts is reached. By default, the user is locked out for two minutes after five failed attempts if the consecutive attempts occur within a ten minute period.

You can change the password policies from the Password Policy Web page, as shown in Figure 71 "Password Policy Web page" (page 144).

Inactive session termination policy

By default, the system suspends a user session after 30 minutes of inactivity. A user must log on to UCM Common Services again when this occurs. Session properties can be managed, as shown in “Editing Session Properties” (page 146).

Logon warning banner

UCM Common Services provides the text for the logon warning banner that a network administrator can change, as shown in “Editing the login warning banner” (page 148).

Access control policies

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of UCM Common Services and the 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 perform 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 UCM Security Services uses the instance and RBAC data model. RBAC identifies the following administrative elements:

- users
- roles
- permissions
- operations
- managed elements

With RBAC, a network administrator can add custom roles to map to specific elements, for example a single CS 1000 element, and then customize permissions for that element.

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

The UCM Security Services 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 Patcher can be granted administration access to All elements of type: Patching Manager.

The following table describes the features supported in the UCM Security Services access control service.

Table 9
Features supported in UCM Security

Feature	Description
Centralized access control policy administration and review	You provision, modify, and review user role and role permission assignments from a central point.
Centralized access control decision point	At run time, RBAC denies or allows the current user to apply certain operations to a managed element from a central point.

Feature	Description
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	You can access only Web pages you are authorized to see. If you try to access an unauthorized site, you receive an HTTP 403 Access Denied Error. Also, if an unauthorized user tries to directly access the business logic layer, for example, through a Web service client, an Access Denied Exception message is sent to the user.

ATTENTION
Roles in CS 1000 are independent of UCM roles. You must separately configure roles for CS 1000 management systems.

Roles and permissions

In the Security branch of the UCM navigation tree, click Roles. On the Roles Web page, users are given permissions to perform tasks. This section describes the two type of roles that UCM Security Services supports–built-in and custom roles.

Built-in roles

UCM built-in roles cannot be deleted and the element and permission mappings cannot be changed by the network administrator. Built-in roles provide authorization to users whose roles are authorized for all the elements of type: x, where x is the type of elements provided for that role. Users who do not require this level of authorization can use custom roles. For more information about custom roles, see “Custom roles” (page 54).

The built-in roles that can be assigned to users are MemberRegistrar, NetworkAdministrator, Patcher, CS1000_Admin1, CS1000_Admin2, CS1000_CLI_REGISTRAR and CS1000_PDT2, as shown in the following table. Within these roles, you have access to various elements and from there you can choose specific permission mappings.

The following is a list of the built-in role permission assignments for UCM Security Services.

Table 10
Built-in roles

Built-in role types	Description
NetworkAdministrator	NetworkAdministrator role provides full privileges on the system. With this role, you have emergency account access to any system including situations when the primary server is down. Use the NetworkAdministrator role where the administrative users are authorized for all roles on all UCM elements with all permissions. Otherwise, it is best practice for the administrator to create separate administrative roles for managing UCM elements and services other than UCM security policies, roles, and users. The NetworkAdministrator role should be used for managing only UCM security. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Hyperlink • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Network Routing Service • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: Snmp Manager • All elements of type: Subscriber Manager The following hidden permissions are granted to the NetworkAdministrator role and cannot be copied to another role: • PERM_QuantumSecurityAdmin: Permission to perform UCM Security Administration operations • PERM_PkiAdmin: Permission to perform PKI administration operations • PERM_AddElement: Permission to add new element instances • PERM_DeleteElement: Permission to delete element instances • PERM_EditElement: Permission to modify existing element instances

Built-in role types	Description
MemberRegistrar	The MemberRegistrar role provides limited access. With this role, you can register new members to the primary server. You have access to the following elements: • All elements of type: IPSec Manager • All elements of type: LinuxBase
Patcher	The Patcher role provides access to software maintenance functions such as patching and maintenance. You have access to the following elements: • All elements of type: Linux Base • All elements of type: Patching Manager
CS1000_Admin1	The CS1000_Admin1 role provides unrestricted OAM access to most administrative functions (except security and account administration) and provisioning for all customers on all call servers and related elements. The role also includes basic diagnostic (PDT1) privileges and access to UCM network-level services for deployment, patching, and SNMP management for CS 1000 systems. Use the CS1000_Admin1 role where the administrative users are authorized for all roles on all UCM elements with all permissions. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Snmp Manager As this role gives permissions to All elements of type: Linux Base, this role is not recommended to users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users. For more information, see “Custom roles” (page 54).

Built-in role types	Description
CS1000_Admin2	The CS1000_Admin2 role provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server elements. The role also includes basic diagnostic (PDT1) privileges and access to UCM network-level services for deployment, patching, SNMP, IPsec and SFTP management for CS 1000 systems. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: Snmp Manager As this role gives permissions to All elements of type: Linux Base, this role is not recommended to users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users. For more information, see “Custom roles” (page 54).
CS1000_PDT2	The CS1000_PDT2 role provides full diagnostic and operating system access to all call servers. It restricts access to administrative functions and customer provisioning data unless combined with another role. You have access to the following elements: • All elements of type: CS1000
CS1000_CLI_REGISTRAR	The CS 1000 Command Line Registrar role provides permission to register and unregister individual CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI. The role has a single permission value to allow or deny a user to register or unregister an element. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Linux Base

Built-in role types	Description
	Users assigned to this role do not have CS 1000 security or Network level security privileges. This role is intended specifically for installation and repair technicians.

Custom roles

On the Roles Web page, a network administrator can create a custom role to map to specific elements and specify custom permissions for that element. Security policy best practices for managing UCM administrative users suggests that the network administrator create custom roles for any users whose roles are not authorized on one or more individual elements of any UCM element type.

For larger CS 1000 systems and for larger enterprise networks of CS 1000 systems of any size, security policy best practice suggests using UCM custom roles for the purposes of limiting administrative user permissions only to the UCM elements on which they are authorized to perform OAM or diagnostic tasks and procedures.

Users whose roles are limited to managing only CS 1000 systems or CS 1000 systems located in a given enterprise site or region, custom roles must be created that map to the individual Linux base elements that have been deployed and configured as Signaling Server elements of the CS 1000 systems they are managing. These users must not have built-in roles with permissions of All elements of type: Linux Base.

Assigned users can perform only specific tasks on an element. For example, a custom role that has been created for a single element such as bvwnodes1.ca.nortel.com can only perform specific tasks on that element. There is a specific permissions set that defines what this role allows you to do on that element.

With custom roles, you can create a role to map to specific elements and specify custom permissions for that element. This ensures that assigned users can perform only specific tasks on an element. For example, a role that has been created for User A with permissions to an individual element such as bvwnodes1.ca.nortel.com can only perform specific tasks that are defined from the permission set for that role.

You can also define roles that apply to how elements and element types are hierarchically arranged under user-defined groups. When you create a permission mapping against a selected group, that group is taken into account when determining user permissions. For example, if you create a permission mapping for the custom role Technician against the element type LinuxBase and apply it to Group A, users assigned to the Technician

role can only perform tasks on elements of type LinuxBase, if they are assigned directly to Group A or to any sub-groups contained within Group A.

For more information about creating custom roles, see Adding a custom role.

Inheritance of UCM role-based permissions for Element type of CS 1000

A UCM element of type CS 1000 represents an instance of CS 1000 Element Manager which has been configured to manage a single CS 1000 system and all of its system elements, for example, Call Server, Signaling Servers, SIP Line Gateways, Media Gateway Controllers, Voice Gateway Media Cards, and any other CS 1000 system-level servers or devices.

UCM role-based permissions for CLI access are inherited from the parent CS 1000 type of element for all children Call Server, Media Gateway Controller, and Voice Gateway Media Card system elements.

UCM role-based permissions for Linux Base Manager and Linux CLI are not inherited for Linux base elements that have been deployed and configured to run CS 1000 Signaling Server applications or CS 1000 Element Manager. Therefore, custom roles for users who are authorized to manage only CS 1000 systems must be mapped to permissions on individual Linux base elements that are deployed and configured as CS 1000 system elements.

Permission templates

The built-in permission templates list contains a listing of UCM built-in roles that are applicable to the UCM type of element whose permission mapping is being edited.

For elements of type CS1000, there is an additional template corresponding to a blank set of permissions for a CS 1000 administrative account "with specified OAM privileges". This UCM template corresponds to the previous CS 1000 system-level OAM account with "limited access to overlays password" (LAPW).

You can customize the permission templates when adding a new role. For more information, see Adding a custom role“Adding a custom role” (page 133).

Role mapping and permission evaluation

When adding a custom role, a permission mapping is created against a selected group and evaluated against that group. Permissions are evaluated using the most privileged algorithm. For example, a permission mapping is created for the custom role Technician against the LinuxBase

element type and applied against the group named Belleville. The Technician role now has permissions for the element of type LinuxBase because the Belleville group (including any sub-group of the Belleville group) is associated with the LinuxBase element type. However, if you are assigned directly to the LinuxBase element type without being assigned to a particular group, for example, within the Belleville group hierarchy, this overrides any group specific permission mappings for the LinuxBase element type and you then have access to all LinuxBase element types.

Security server configuration

This chapter describes security server configuration and administrator password reset.

Navigation

Prerequisites

- Ensure Linux base operating system is installed and default Nortel account is configured.
- Ensure the DNS server is configured.
- A local user account must be created before it can be validated.

For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

ATTENTION
Nortel strongly recommends that you do not change the FQDN and host name of the primary and backup security servers after security configuration has been completed. You can change the FQDN of the member security server. For information about changing the configuration on an already configured member server, see"Making changes on a member server" (page 74).

In Base Manager, on the Edit Network Identify page, the Host name and Domain fields in the Fully Qualified Domain Name (FQDN) section cannot be changed as these fields are dimmed.

Security Server configuration

The following procedures describe security configuration of the primary security server, backup security server, and member server. Access UCM by typing https://<FQDN>, where <FQDN> is the Fully Qualified Domain

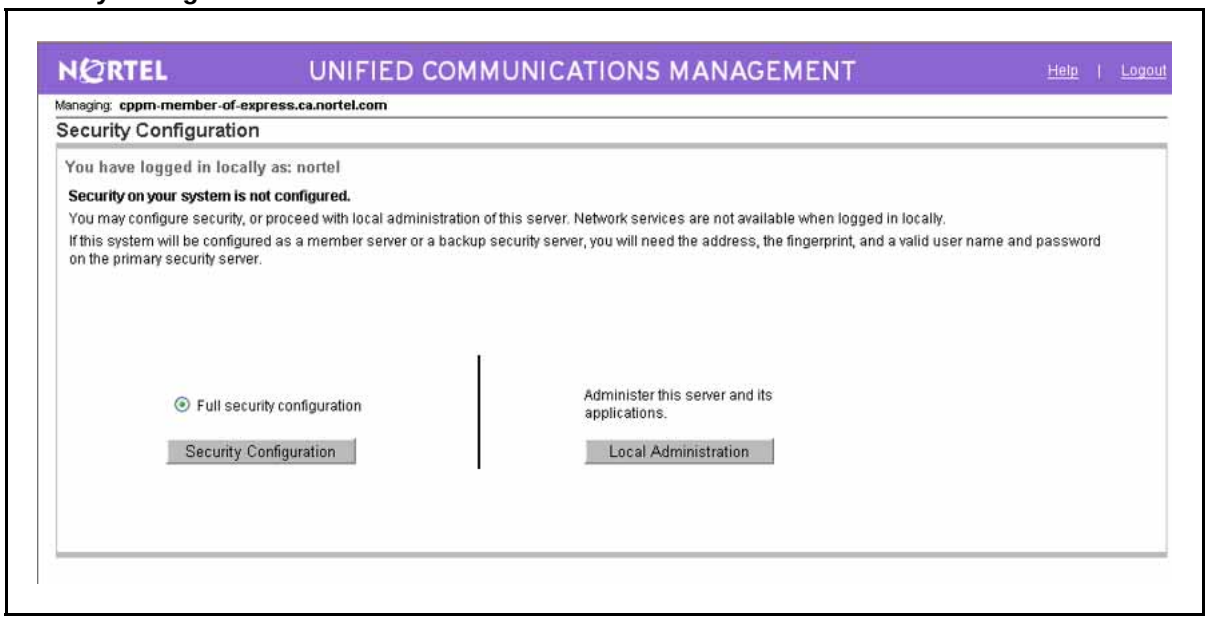
Name. If the server is not configured, the local logon page appears. Log on using the default Nortel account using the password that you specified during the Linux base installation. For more information, see Table 7 "Supported built-in accounts" (page 44).

Configuring the primary security server

You must configure the primary security server on a stand-alone system to provide basic security features such as user administration including password changes from the Web EM, the ability to configure authorization levels, and the enforcement of security policies.

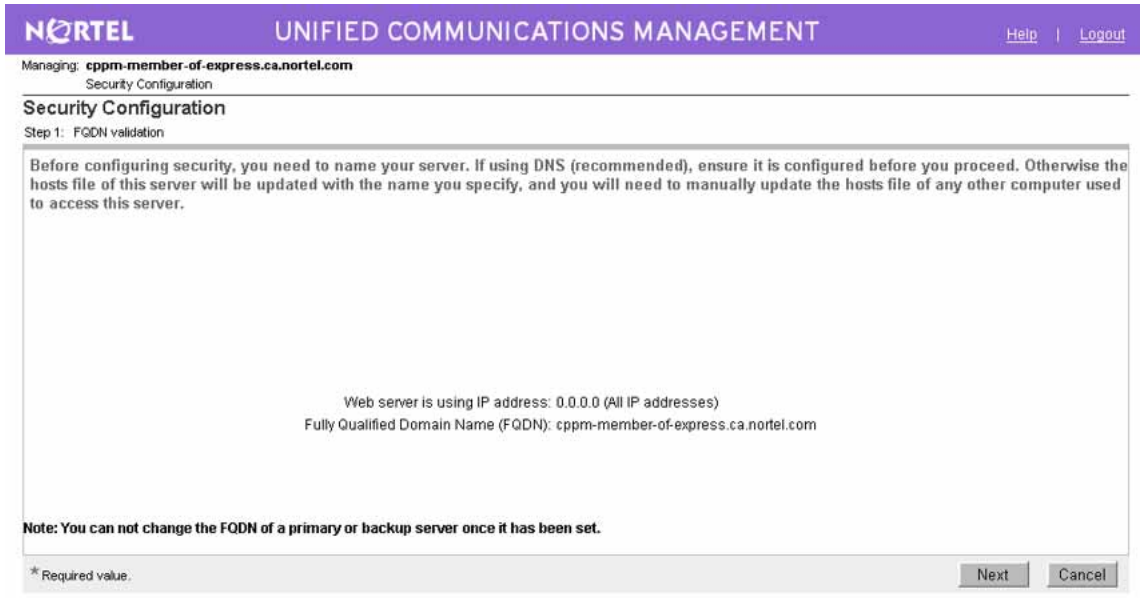
Step	Action
1	In the Web browser **Address** bar, type **https://<FQDN>** of the Primary Security Server and press **Enter**.
2	On the Security Configuration page, select **Full security configuration**, as shown in the following figure.

Figure 7
Security configuration



3	Click **Security Configuration**. The FQDN validation page appears, as shown in the following figure.

Figure 8
FQDN validation

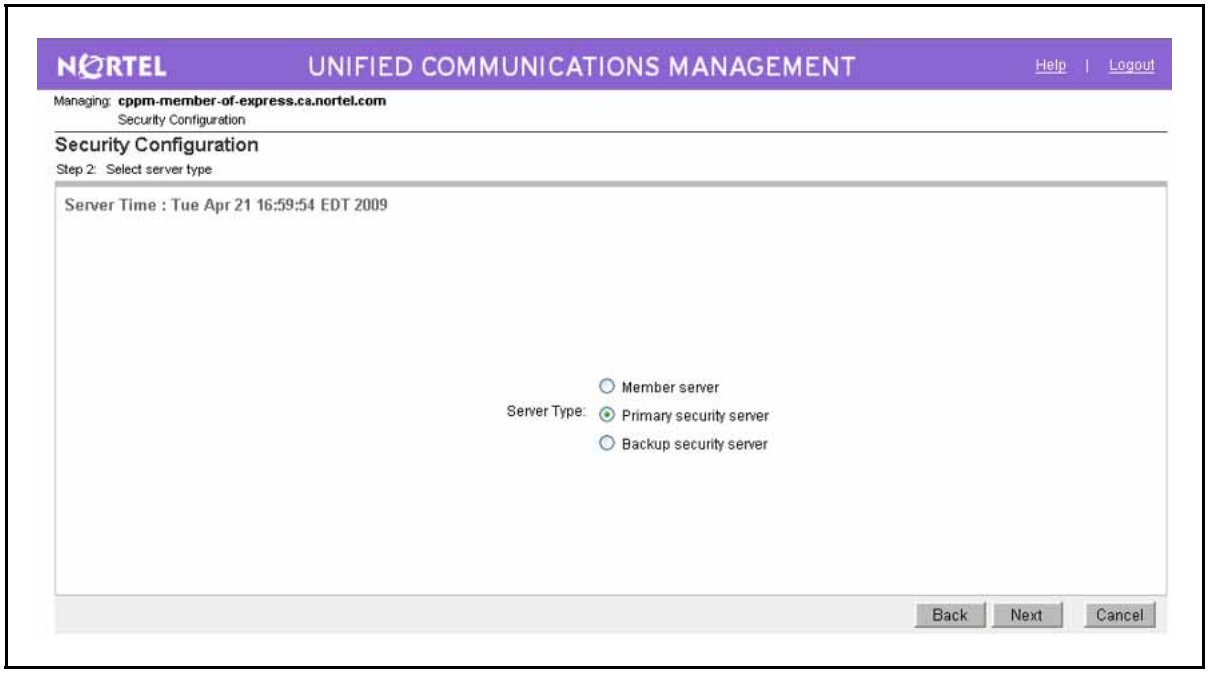


4 Confirm the IP address and FQDN is correct, and click **Next**.

ATTENTION
If using a DNS server, the DNS server must be configured before proceeding.

The Select server type page appears, as shown in the following figure.

Figure 9
Select server type

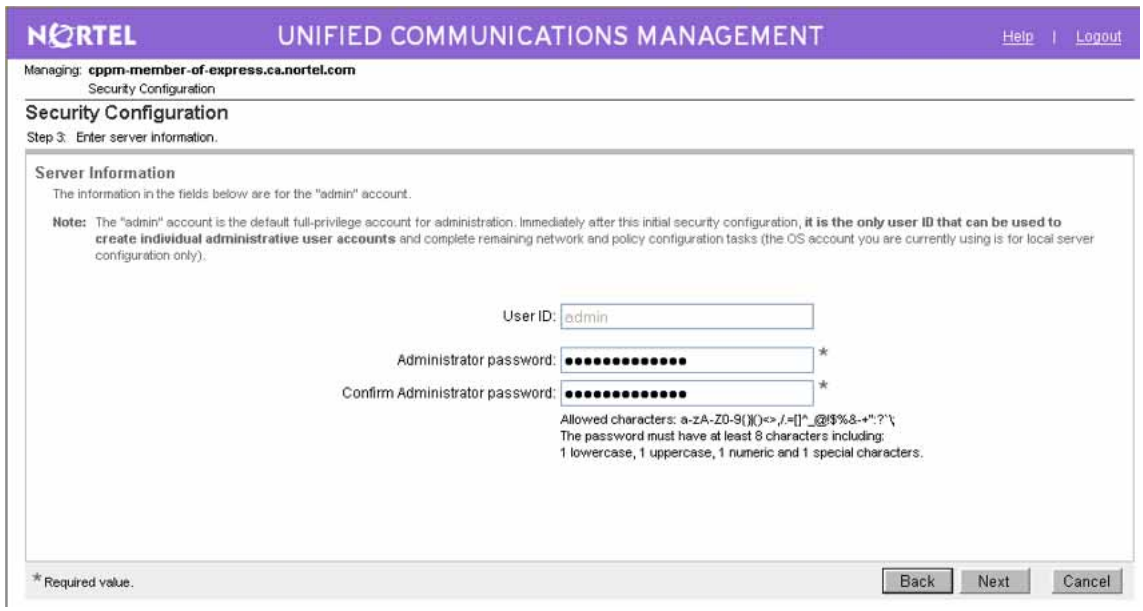


5 Select **Primary security server**, and click **Next**.

The Enter server information page appears, as shown in the following figure.

ATTENTION
When using the admin account to change user account passwords, the user is forced to change their password upon logging on for the first time. During admin account creation, the NetworkAdministrator privilege is provided by default.

Figure 10
Enter server information



6 In the **Administrator password** field for the built-in Admin account, type the new password. The password must contain a minimum of eight characters with.

- at least one number from 0 to 9
- one special character such as an exclamation mark (!)
- one upper- and one lowercase character

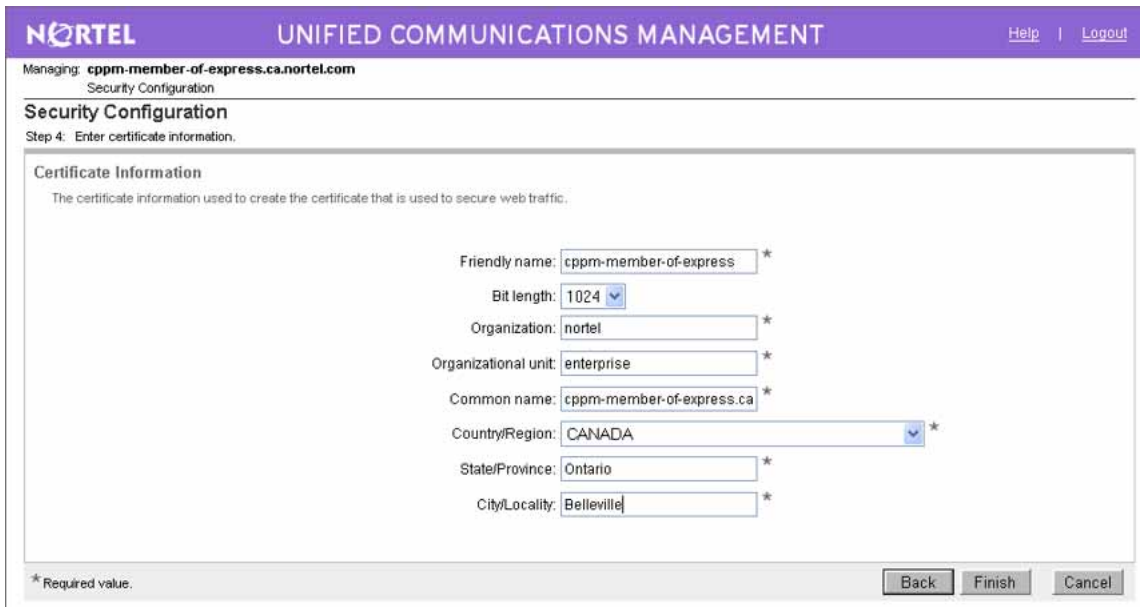
Allowed characters in the password are a-zA-Z0-9{}|()<>,/.=[]^~ _@!'$%&-+":?'\'

7 In the **Confirm Administrator password** field, type the new password.

8 Click **Next**.

The Enter certificate information page appears, as shown in the following figure.

Figure 11
Enter certificate information



9 Configure the following values:

Friendly name: Type a string that would be used to identify the certificate, for example, UCM Primary Security Server.

Bit Length: Type a value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: Select a country from the list.

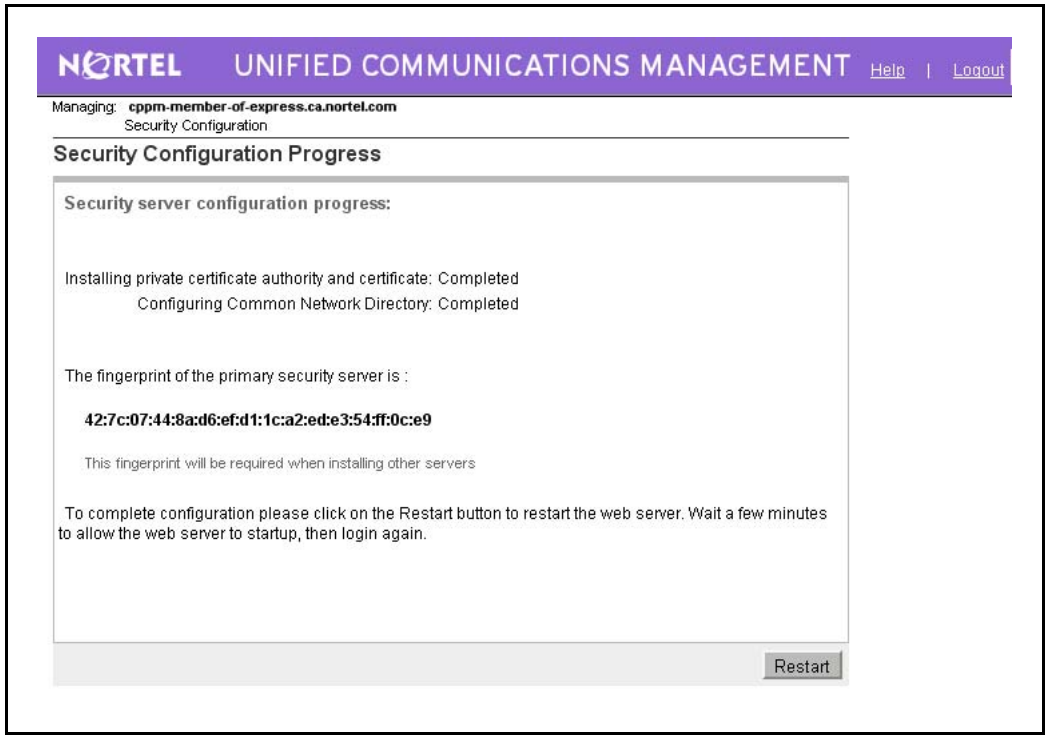
State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

10 Click **Finish**.

The Security server configuration progress page appears, as shown in the following figure.

Figure 12
Security Configuration Progress



11 Click **Restart** to restart the Web server and for the security configuration changes to take effect.

The Restarting the server Web page appears.

ATTENTION
Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart process. The user can log on with the recently configured Administrator password after the Web server restarts.

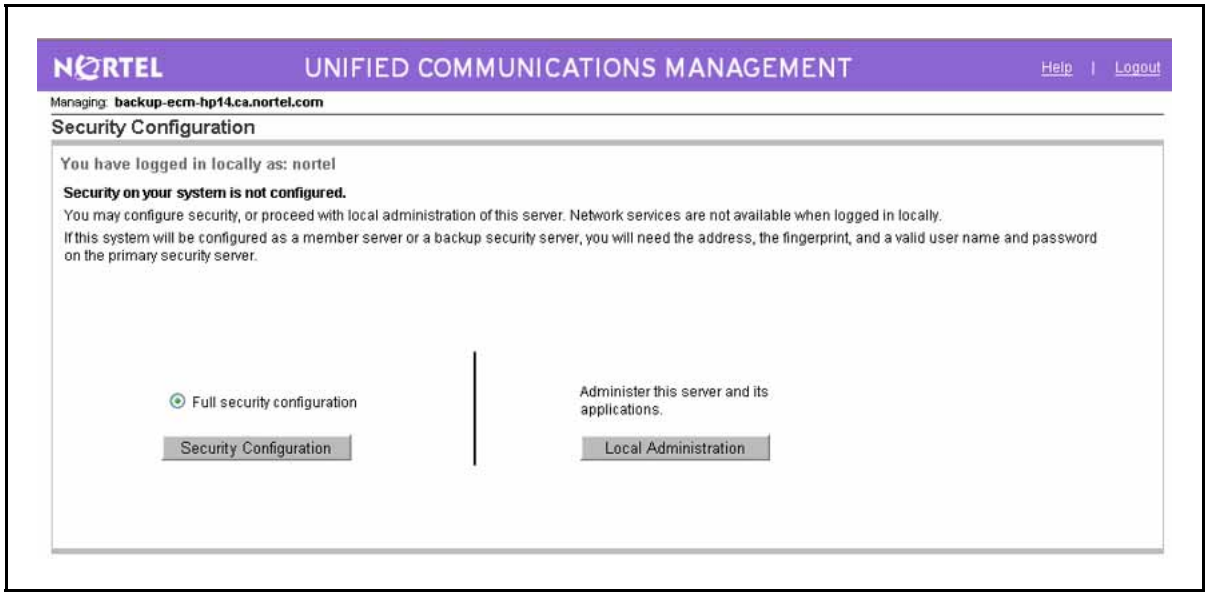
--End--

Configuring a backup security server

The backup security server is an optional server that can be configured to be used for authentication and authorization when the primary security server is unavailable. Use the following procedure to configure the backup security server.

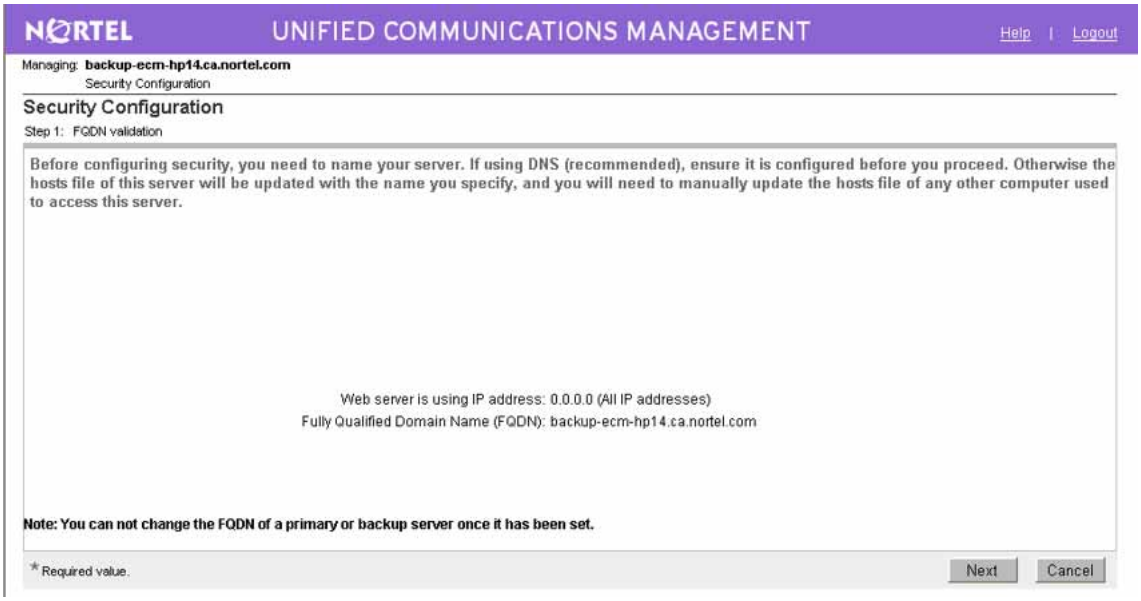
Step	Action
1	In the Web browser address bar, type **https://<FQDN>** of the Backup security server and press **Enter**.
2	On the Security Configuration page, select **Full security configuration**, as shown in the following figure.

Figure 13
Security Configuration



3	Click **Security Configuration**. The FQDN validation page appears, as shown in the following figure.

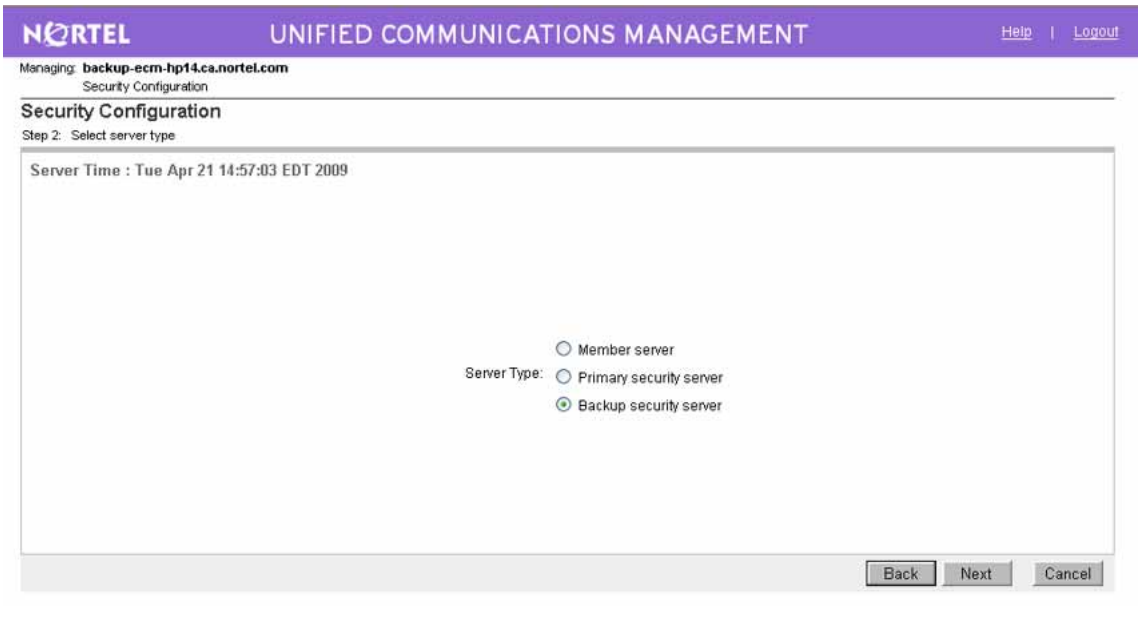
Figure 14
FQDN validation



Click **Next**.

The Select server type page appears, as shown in the following figure.

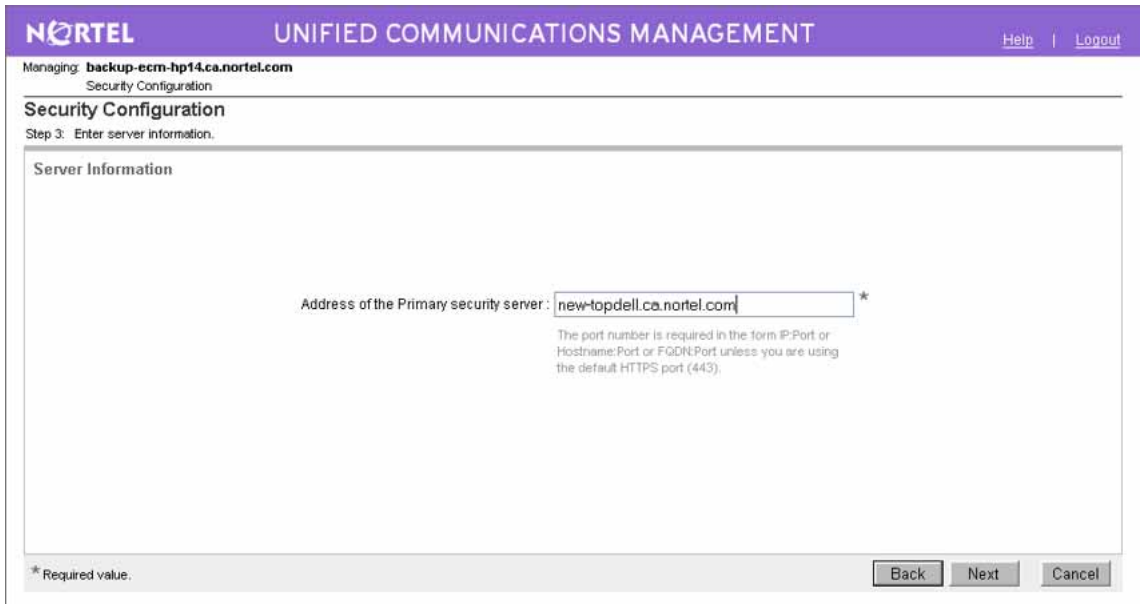
Figure 15
Select server type



Select Backup security server and click **Next**.

The Enter server information page appears, as shown in the following figure.

Figure 16
Enter server information

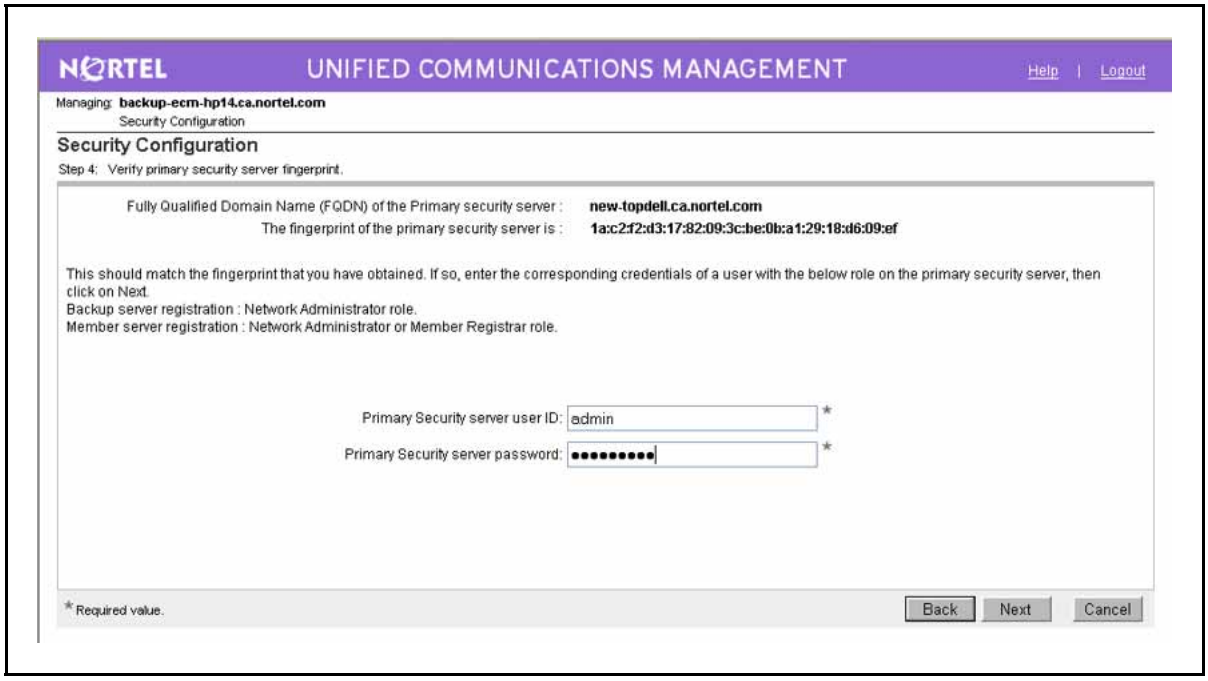


4 Confirm the FQDN of the Primary security server is correct, and click **Next**.

ATTENTION
If using a DNS server, the DNS server must be configured before proceeding.

The Verify primary security server fingerprint page appears, as shown in the following figure.

Figure 17
Verify primary security server fingerprint

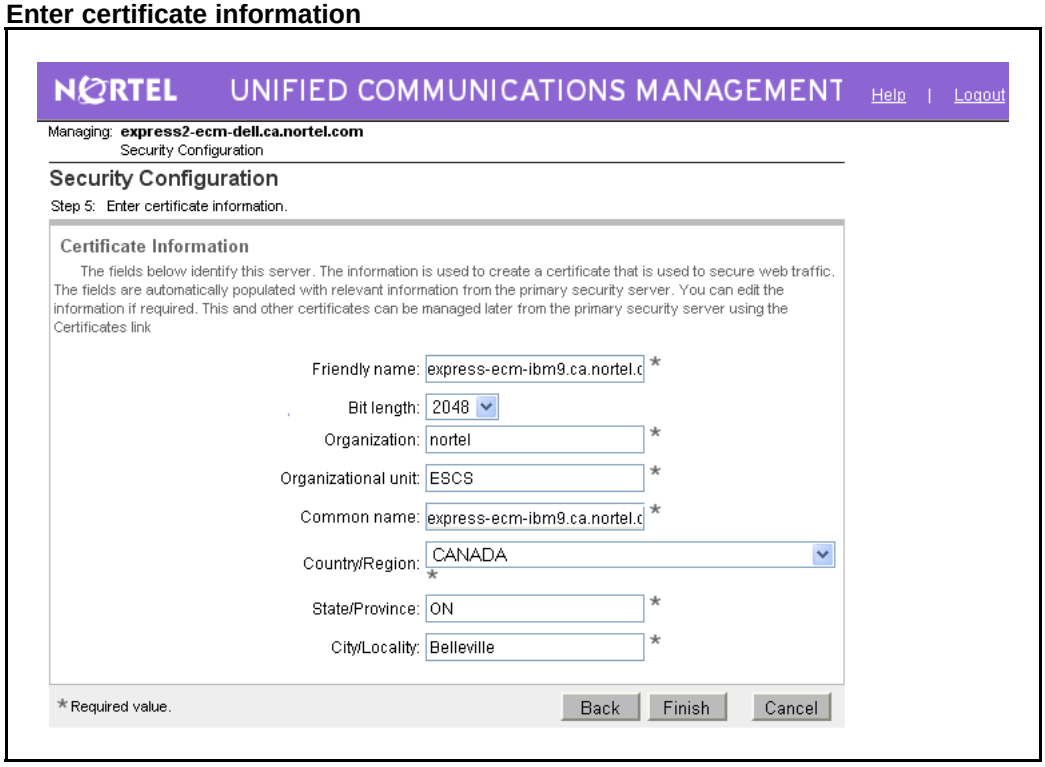


5 Verify the FQDN and fingerprint of the primary security server. If it is valid, type a Primary Security server user ID with the NetworkAdministrator role and password, and click **Next**.

ATTENTION
The primary security server must be configured and running. The Primary Security server user ID is any administrator account that has NetworkAdministrator role assigned.

6 The Enter certificate information window appears, as shown in the following figure.

Figure 18
Enter certificate information



7 The following values are populated from the Primary security server. You can accept the selected options or change them.

Friendly name: A string that would be used to identify the certificate, for example, UCM Backup Security Server.

Bit Length: A value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: A Country/Region where the primary server is located.

State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

8 Click **Finish**.

The Security server configuration progress page appears, as shown in Figure 12 "Security Configuration Progress" (page 63).

9 Click **Restart** to restart the Web server for the security configuration changes to take effect.

ATTENTION
Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart. You can log on with the recently configured Administrator password after the Web server restarts.

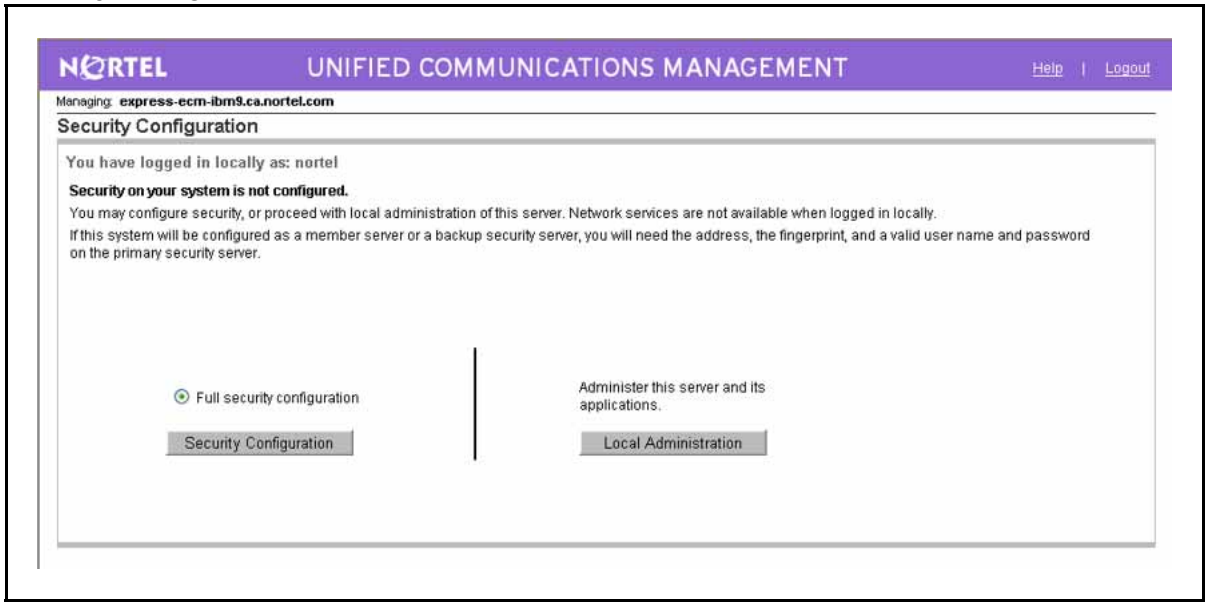
--End--

Configuring a member server

Configure the member security server.

Step	Action
1	In the Web browser **Address** bar, type **https://<FQDN>** of the Member security server and press **Enter**.
2	On the Security Configuration page, select **Full security configuration**, as shown in the following figure.

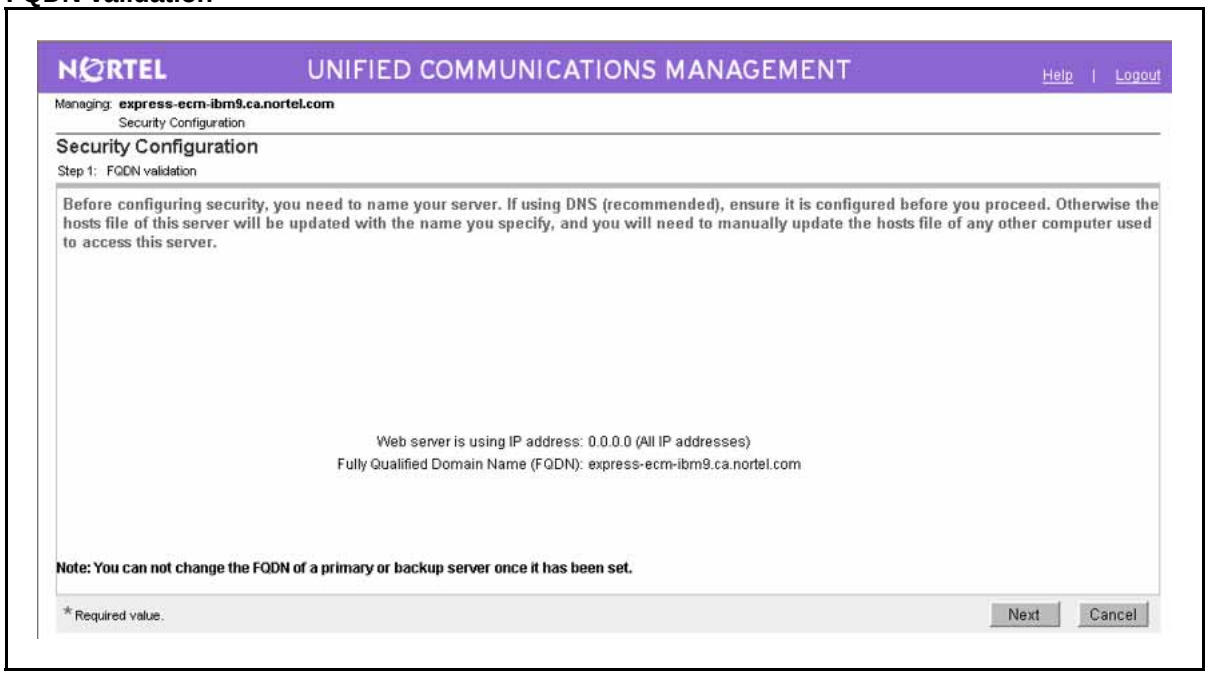
Figure 19
Security Configuration



3 Click **Security Configuration**.

The FQDN validation page appears, as shown in the following figure.

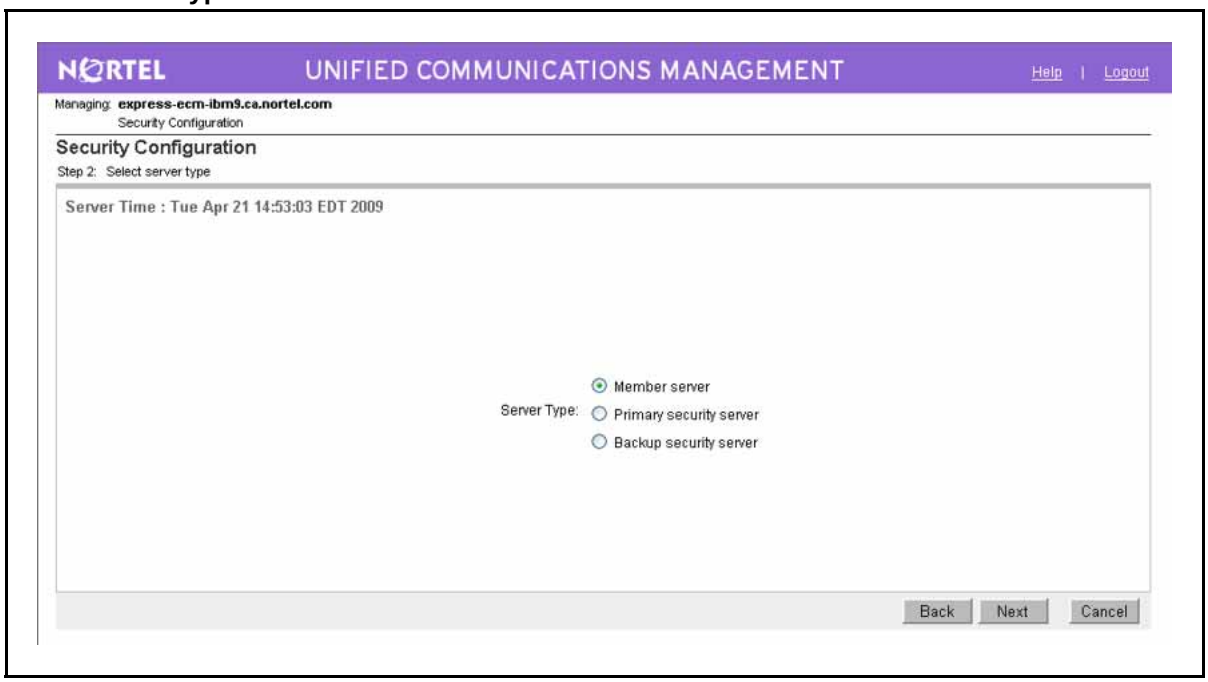
Figure 20
FQDN validation



4 Click **Next**.

The Select server type page appears, as shown in the following figure.

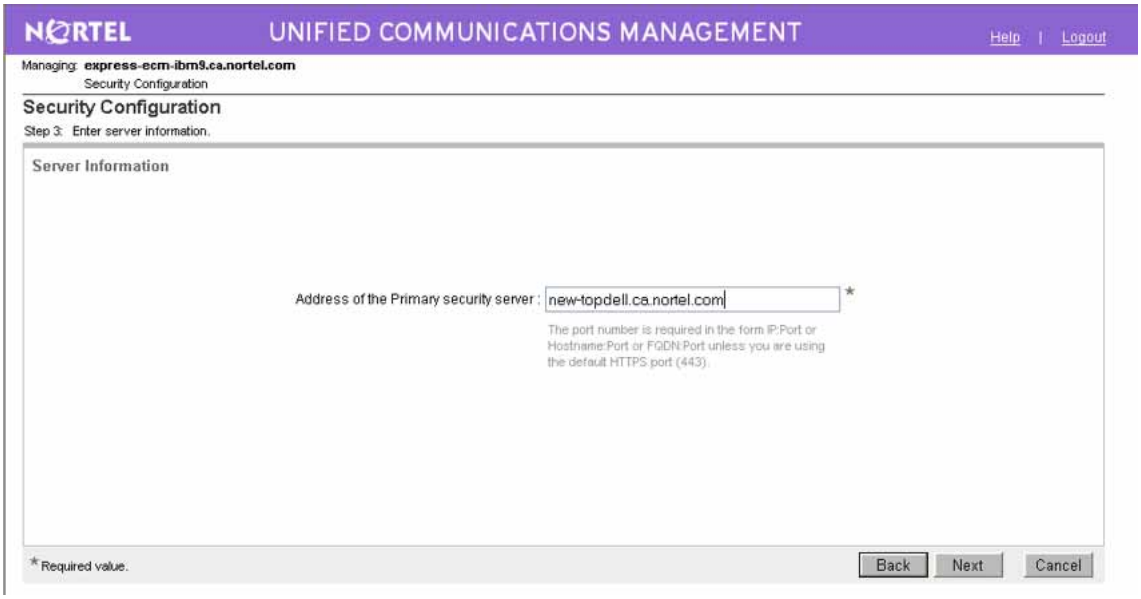
Figure 21
Select server type



5 Select **Member server**, and click **Next**.

The Enter server information page appears, as shown in the following figure.

Figure 22
Enter server information

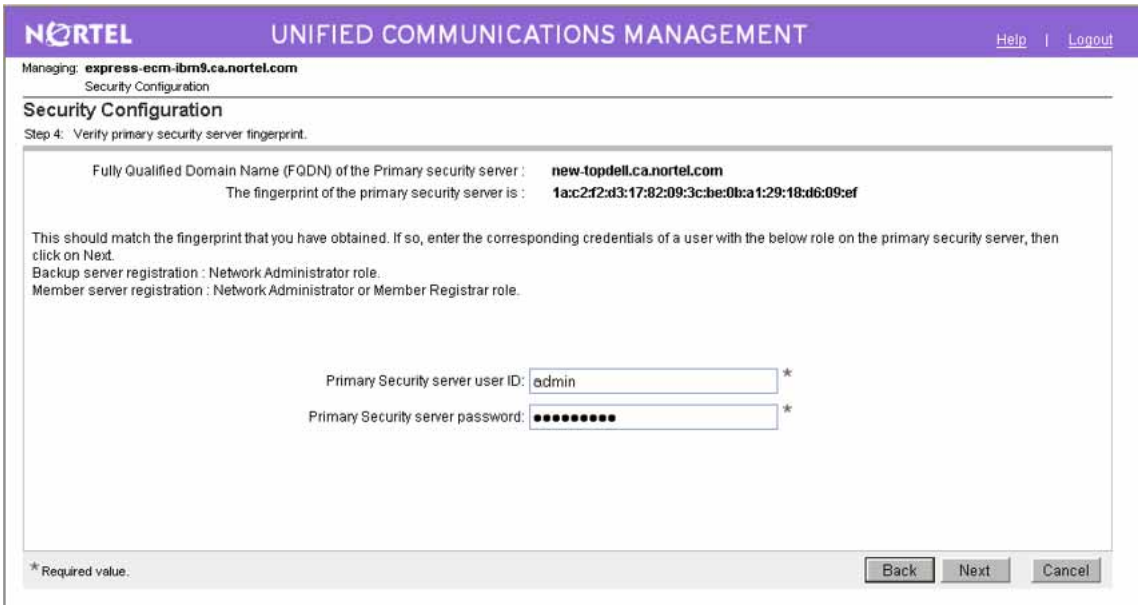


6 Confirm the FQDN of the Primary security server is correct, and click **Next**.

ATTENTION
The primary security server must be configured and running.

The Verify primary security server fingerprint window appears, as shown in the following figure.

Figure 23
Verify primary security server fingerprint

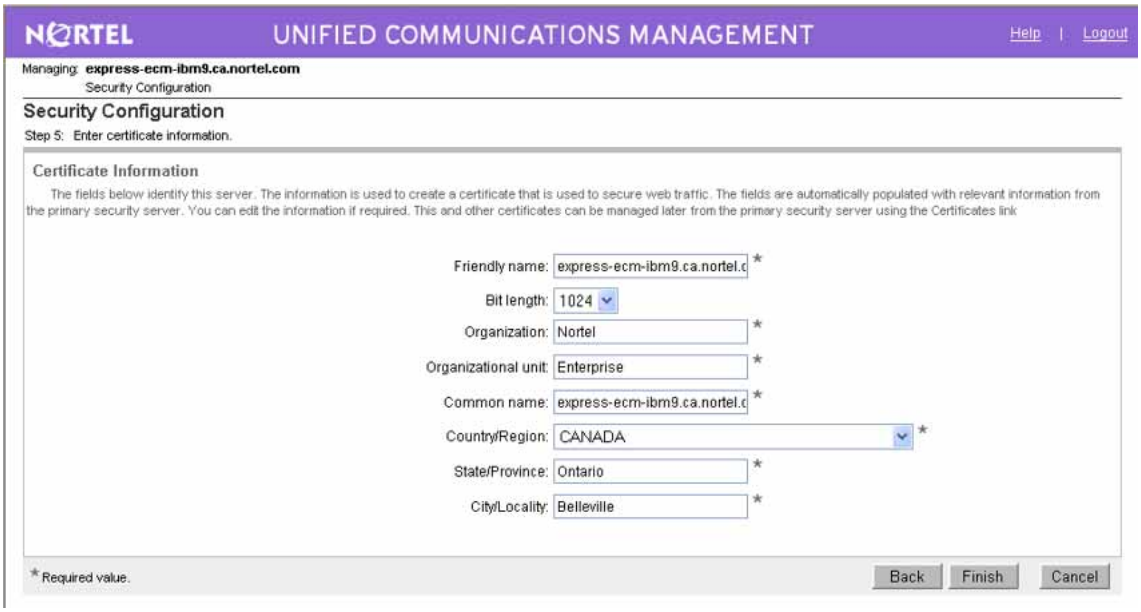


7 Verify the FQDN and fingerprint of the primary security server. If it is valid, type a Primary Security server user ID with the network administrator role and password, and click **Next**.

ATTENTION
The primary security server must be configured and running. The Primary Security server User ID is any administrator account that has the NetworkAdministrator role assigned.

The Enter certification information window appears, as shown below.

Figure 24
Enter certificate information



8 The following values are populated from the Primary security server. You can accept the selected options or change them.

Friendly name: A string that would be used to identify the certificate, for example, UCM Backup Security Server.

Bit Length: A value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: A Country/Region where the primary server is located.

State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

9 Click **Finish**.

The Security server configuration progress window appears, as shown in Figure 12 "Security Configuration Progress" (page 63).

10 Click **Restart** to restart the Web server for the security configuration changes to take effect.

ATTENTION
Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart. You can log on with the recently configured Administrator password after the Web server restarts.

--End--

For information about changing the configuration of a member server, see "Making changes on a member server" (page 74).

Security configuration changes

You can make configuration changes to the member server. The following procedure describes the steps to change the Fully Qualified Domain Name (FQDN), change the certificate information, point to a different primary server, and demote a primary and backup server.

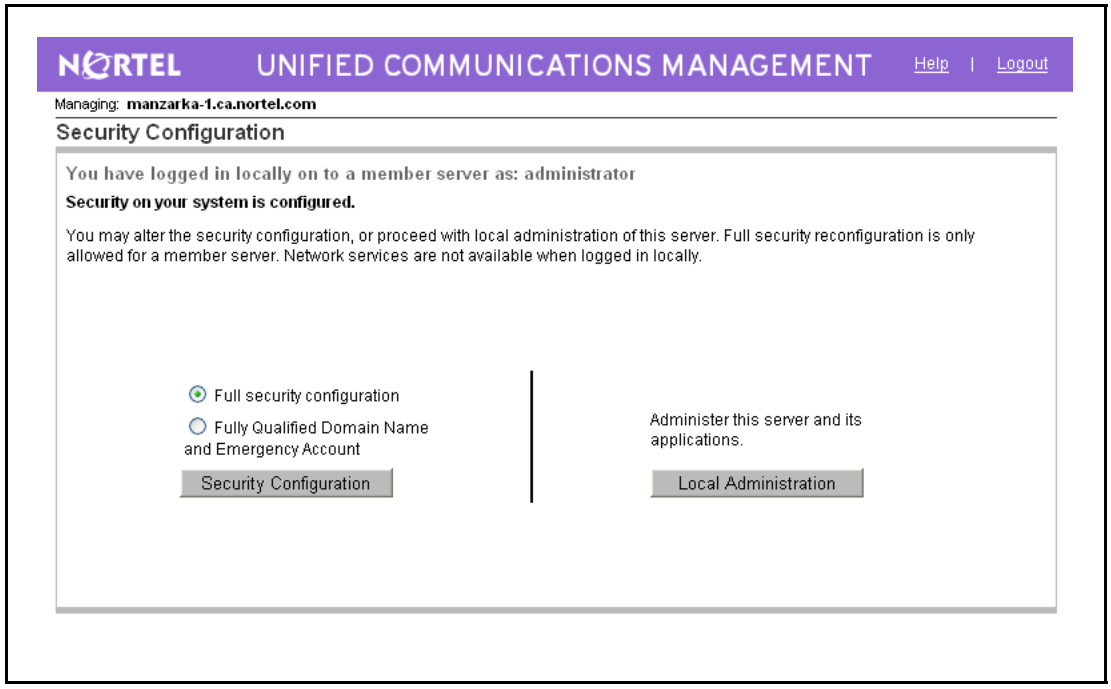
ATTENTION
Certificates are managed from the security server at the network level. You must restart the Web server after you save the changes.

Making changes on a member server

ATTENTION
The primary and backup server cannot be reconfigured. You cannot promote a member server to a primary server. A fresh installation is required if you want to change a member server to a primary server.

Step	Action
1	Go to the local logon page of an already configured member server, as shown in the following figure.

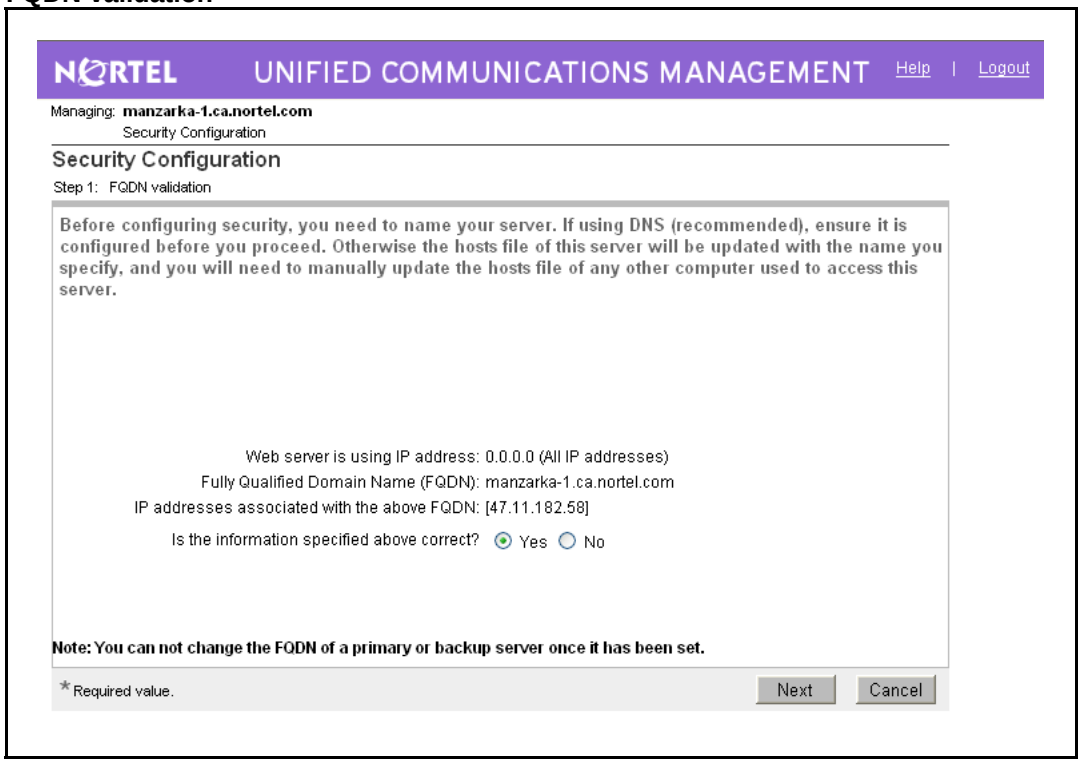
Figure 25
Security configuration



2 Select **Full security configuration**, and click **Security Configuration**.

The FQDN validation page appears, as shown in the following figure.

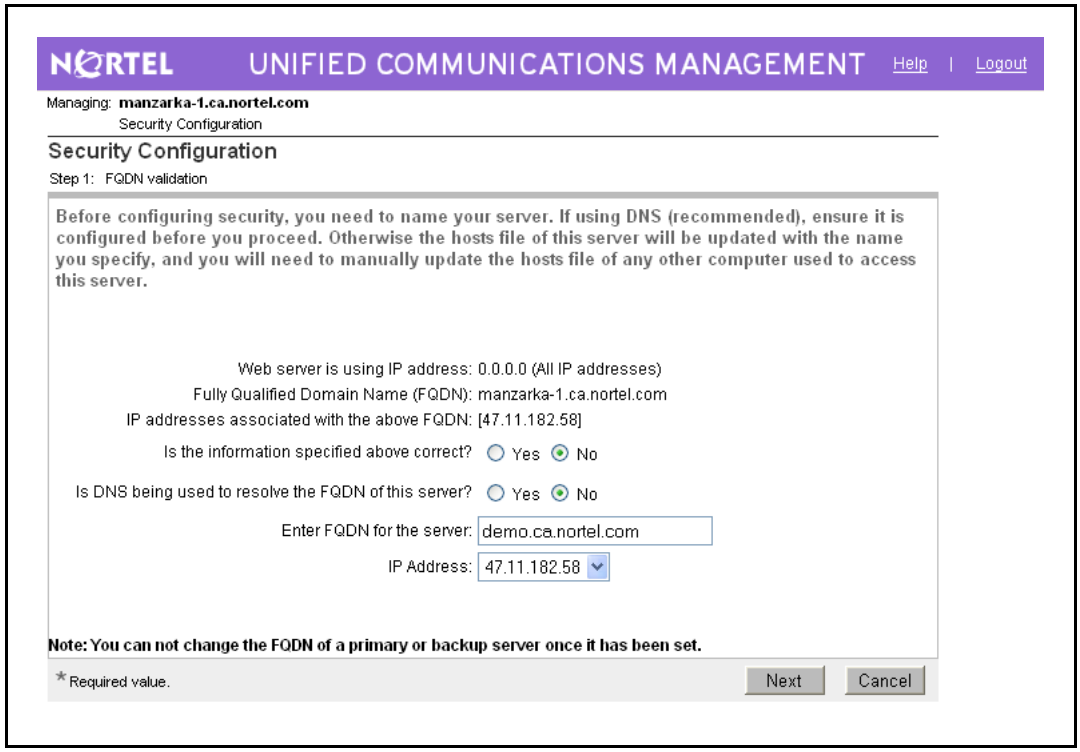
Figure 26
FQDN validation



3 Select **No**, and click **Next**.

The FQDN validation page refreshes allowing you to make changes, as shown in the following figure.

Figure 27
Refreshed FQDN page



4 Type the new FQDN and IP address of the member server, and click **Next**.

The Select server type page appears.

5 Select **Member server**, and click **Next**.

6 Continue to follow Step 6 to Step 10 in “Configuring a member server” (page 69).

--End--

Configuration failure

Failed configuration attempts are identified in the Status field. Click **Try again** to clear the previous configuration attempt and to begin a new configuration attempt. The new configuration attempt begins at the Primary security server from the Security Configuration Server Information page as shown in Figure 10 "Enter server information" (page 61). Partial configurations are not supported.

Demoting a primary and backup server

The UCM primary and backup security server can be demoted to a member server in a new domain. The security domain of the demoted primary server is no longer valid so existing backup servers must also be

demoted to member servers in the new domain. The security configuration of any existing member servers must be reconfigured to a primary server in another domain, see “Security configuration changes” (page 74).

Prerequisites:
You must be logged on locally to the primary security server as Administrator.

Step	Action
1	From the Security Configuration page, click **Demote Security Server** and click **Security Configuration**. The FQDN validation page appears.
2	Select **No**, and click **Next**. The FQDN validation page refreshes allowing you to make changes.
3	Type the new FQDN and IP address of the member server or backup server, and click **Next**. The Select server type page appears.
4	Select **Member server** or **Backup server**, and click **Next**.
5	Continue to follow Step 6 to Step 10 in “Configuring a member server” (page 69).

--End--

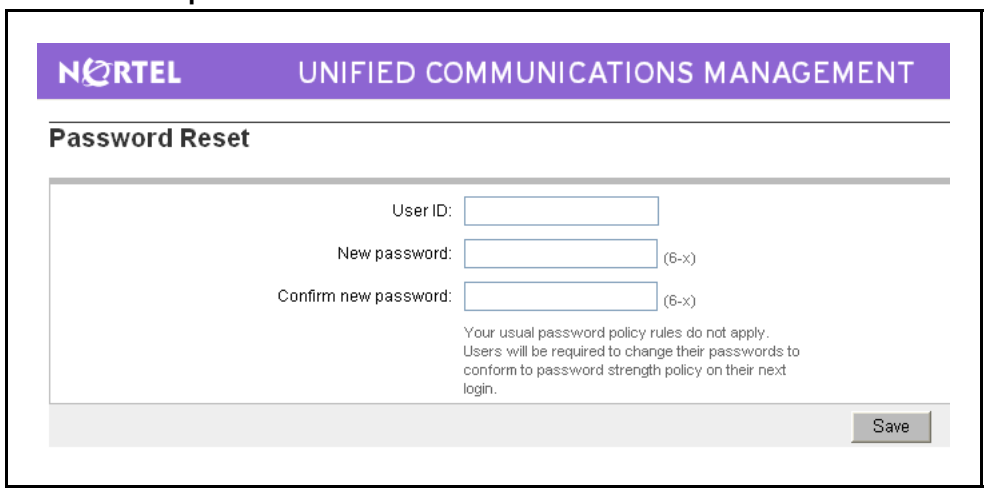
Resetting an Administrator password

If the Administrator password is forgotten or the account is locked out, the password can be reset from the user interface. Use the following procedures for logging on to the local logon page with an emergency account.

Step	Action
1	In the Web browser **Address** bar, type **https://<FQDN>/local-login** of the Primary Security Server and press **Enter**.
2	Log on using the default emergency account or Nortel account. For more information, see “Built-in account” (page 44). The Security Configuration page appears, as shown in Figure 25 "Security configuration" (page 75).
3	In the Web browser **Address** bar, type **https://<FQDN>/passwordReset** of the Primary Security Server and press **Enter**.

The password reset page appears, as shown in the following figure.

Figure 28
Administrator password reset



4 In the **User ID** field, type the User ID for the password you want to reset.

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

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

7 Click **Save**.

A confirmation page appears when you change the password.

--End--

Logon and logoff options in UCM

This chapter describes logging on to UCM for the first time and changing your password, and other log on and log off options in UCM.

Navigation

Logon modes in UCM

Use the following procedures to log on to UCM using the central or network logon mode and switching from network logon mode to central logon mode.

Central logon mode

Nortel recommends logging on to UCM by entering the FQDN. This is called central logon mode. Central logon supports SSO, centralized access control, password changes, resets, and password expiry notices. You can also manage network resources.

The password reset page appears when logging on for the first time, after a password reset, and when your password is about to expire.

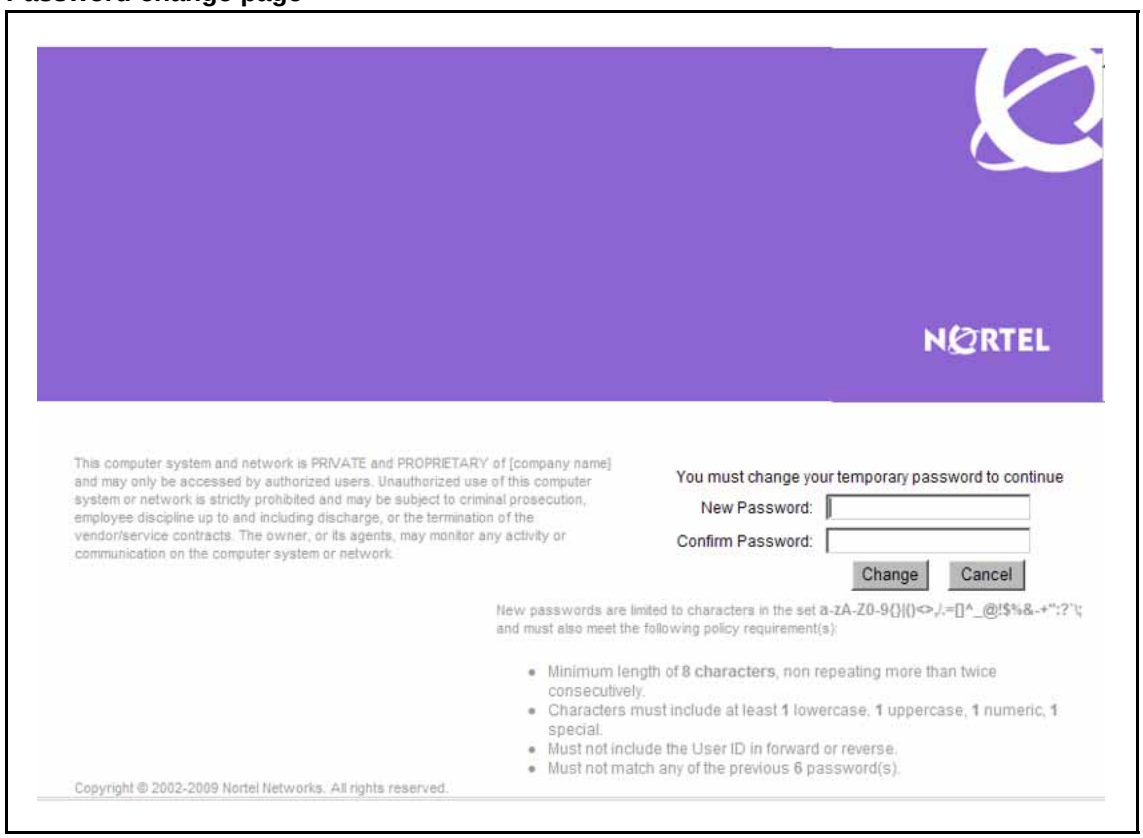
ATTENTION
Nortel recommends using the central logon mode (FQDN) for UCM.

Logging on to UCM in Central logon mode for the first time

Use the following procedure to log on to UCM for the first time using central logon mode.

Step	Action
1	In the Web browser **Address** bar, type **https://<FQDN>** and press **Enter**. For example, https://primary.ca.nortel.com.
2	Type a valid User ID and password.
3	The password change page appears, as shown in the following figure.

Figure 29
Password change page



4	Type your new password and confirm your password by typing it again and click **Change**.

--End--

Logging on using the FQDN in central logon mode

Log on to UCM using the central logon page by entering the FQDN. Central logon supports SSO, centralized access control, and password changes and resets. You can also manage network resources with central logon.

Step	Action
1	In the Web browser **Address** bar, type **https://<FQDN>** and press **Enter**. For example, https://primary.ca.nortel.com.
2	Type a valid User ID and password.
3	On the **Elements** page, click an element item. When the element management URL is on a different UCM, the user is redirected to the Web page of the selected element without reauthentication.

--End--

Network logon mode

Log on to UCM by entering the IP address. This is called network logon mode. SSO and Kerberos based SSO with Microsoft Windows is not supported when you log on from the network logon page. Failover works in network logon mode when the primary server is down. The member server redirects you to the backup security server. Network logon can also manage network resources and supports centralized access control. The administrator cannot change or reset passwords in network logon mode.

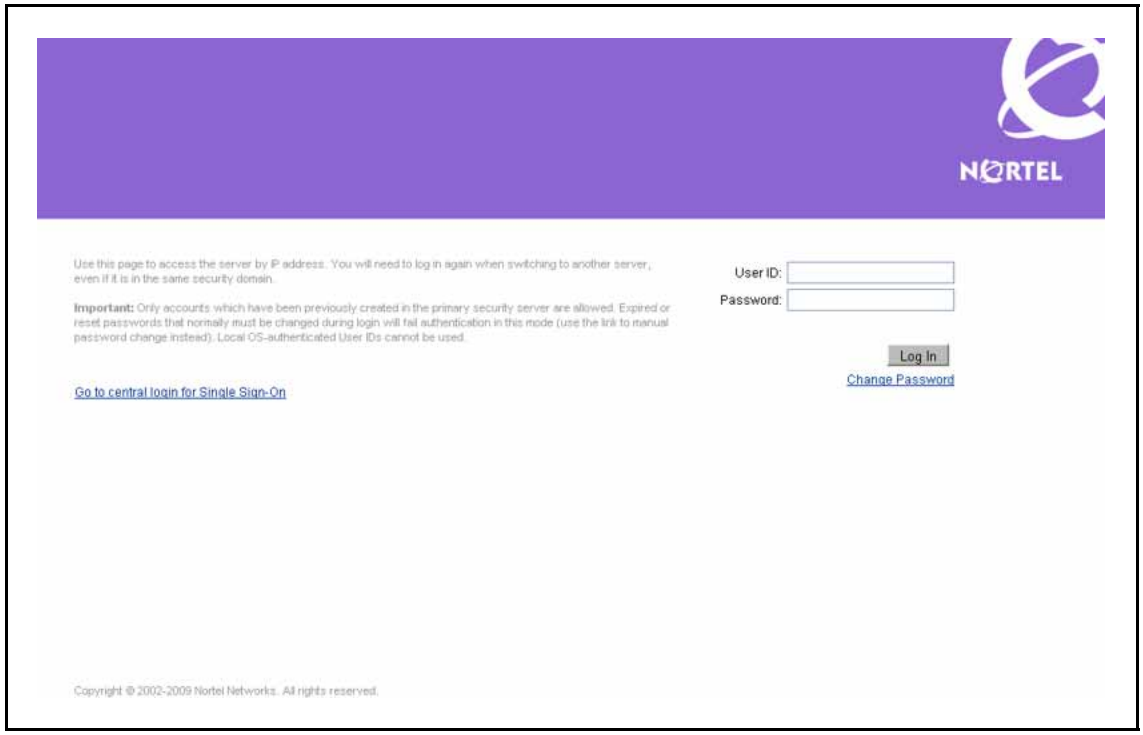
Logging on to UCM in Network logon mode for the first time

If logging on to UCM for the first time in Network logon mode, you must manually change the default password.

Follow the default password strength policy as defined by the administrator. For more information, see "The password strength policy enforcement" (page 47).

Step	Action
1	Open the Web browser.
2	Type the IP address in the **Address** bar, and press **Enter**. The Logon Web page appears, as shown in the following figure.

Figure 30
Logon Web page

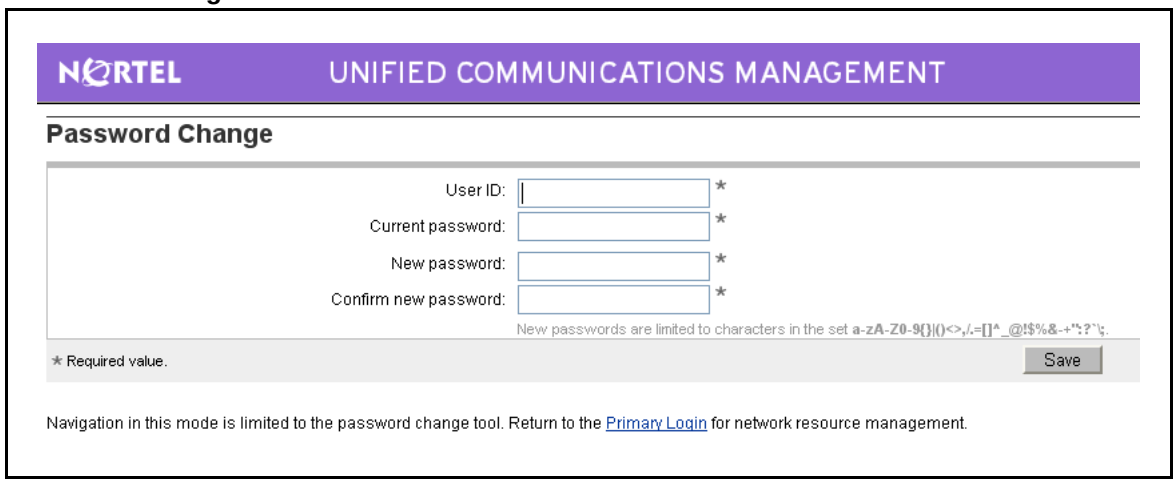


3 Click **Change Password**.

ATTENTION
If you attempt to logon using your temporary password, you will receive the error message "Login error. Please check your username and password." You must click the Change Password link before logging on for the first time.

The Password Change screen appears.

Figure 31
Password Change



ATTENTION
User IDs in UCM are not case-sensitive. However, Linux-based User IDs that are independent of UCM are case-sensitive.

4 Type the following information:

- User ID
- Current password
- New password
- Confirm password

5 Click **Save**.

--End--

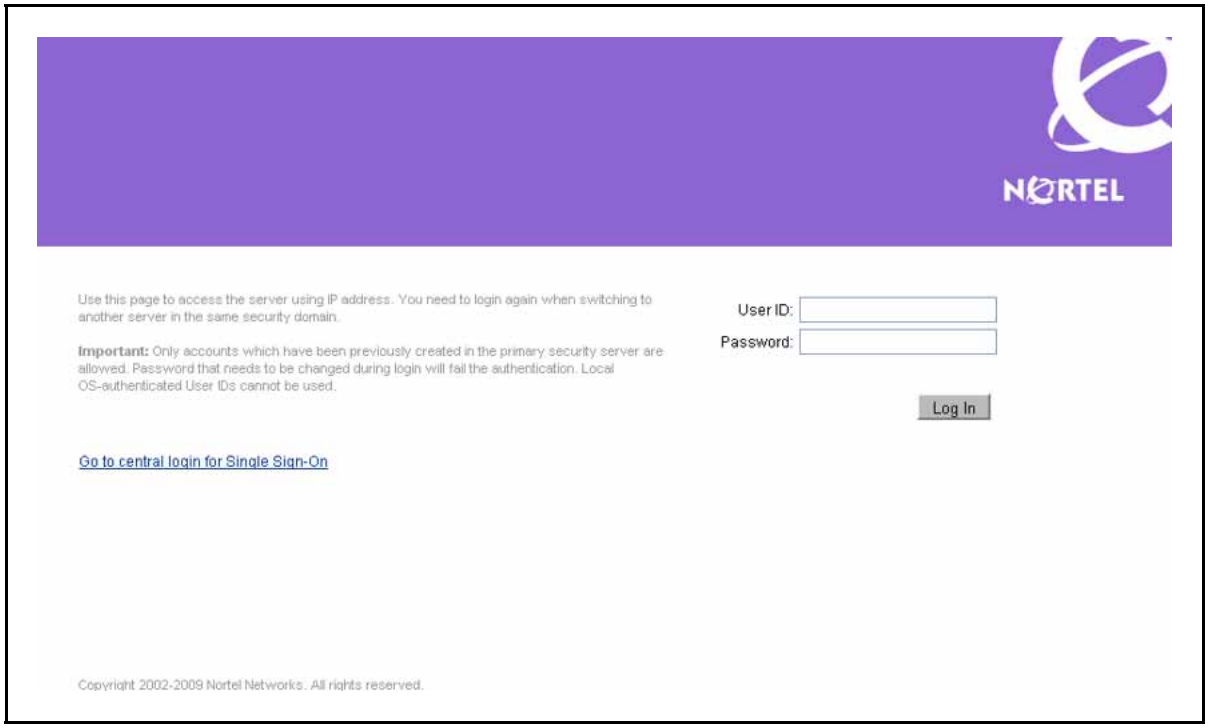
ATTENTION
On the Internet Explorer browser, you may see a digital certificate pop-up. To disable, see "Disabling digital certificate pop-up" (page 87).

Logging on using the IP address in network logon mode

Log on to UCM using the network logon page by entering the IP address. Nortel recommends using central logon mode. For more information, see "Logging on using the FQDN in central logon mode" (page 83).

Step	Action
1	In the Web browser **Address** bar, type the IP address of the Primary Security Server, and press **Enter**. The Logon Web page appears, as shown in the following figure.

Figure 32
Network logon page



2 Type a valid User ID and password at the network Logon page.

3 Click **Login**.

The application Web page appears.

4 Click the link of an element in the same Web browser window.

If an element is installed on the same UCM, the selected element Web page appears without reauthentication.

--End--

Switching from network logon mode to central logon mode

Switch from network logon mode to central logon mode to allow for Single Sign-On.

Step	Action
1	In the Web browser **Address** bar, type the IP address of the Primary Security Server, and press **Enter**.
2	Click **Go to central login for Single Sign-On**.
3	Type a valid User ID and password at the central Logon page.
4	Click **Login**.

You do not have to reauthenticate to switch between Web servers in the same security domain.

--End--

Disabling digital certificate pop-up

Disable digital certificate pop-ups from Internet Explorer when no certificates are listed during logon attempt.

Step	Action
1	On the Internet Explorer browser, choose **Tools, Internet Options**.
2	Select the **Security** tab and click **Custom Level**.
3	Scroll to select the option **Don't prompt for client certificate selection when no certificate or only one certificate exists** and click **Enable**.
4	Click **OK**.
5	Click **Yes** at the prompt "Are you sure you want to change the settings for this zone?".

--End--

SSO using FQDN without DNS infrastructure

The FQDN uses an IP address with DNS. To use SSO for Web access without DNS infrastructure, you must include the FQDN in the local **`\winnt\system32\drivers\etc\hosts\etc\hosts`** file on your computer.

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

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

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

Logoff options

The following table describes how to log off UCM Common Services and how to log off globally for elements within the same or different UCM system.

Table 11
Logoff options in UCM

Logoff method	Action	Result
Log off UCM Common Services	Click Logout at the top right corner of the window.	A Web page appears confirming the logoff 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 the same UCM server.	You are redirected to the UCM logon Web page.
Log off globally for Web applications in a different UCM	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 UCM server.	You are redirected to the UCM logon Web page.
Session or idle timeout	You are automatically logged off when the maximum session or idle time is reached.	You are redirected to the UCM logon Web page.

ATTENTION
You can log on multiple times using the same User ID. If you close the UCM Web page window without clicking Logout, you can log on to a new session with the same User ID. The previous Logon session is no longer accessible and continues to use resources until the idle timeout period is reached. Nortel recommends that you click Logout to end your session.

UCM Network configuration

This chapter contains information about managing elements in UCM Common Services. The Elements page is the default Web page when you log on to UCM. The Elements page has two views: table view and tree view. For more information about the views, see “Table view” (page 20) and “Tree view ” (page 20).

This chapter covers the following topics:

Navigation

Elements

The following sections contain procedures to manage elements by using the tree or table view.

Manage elements using the edit navigation tree

Perform the procedures in the following sections to manage the elements using the navigation tree.

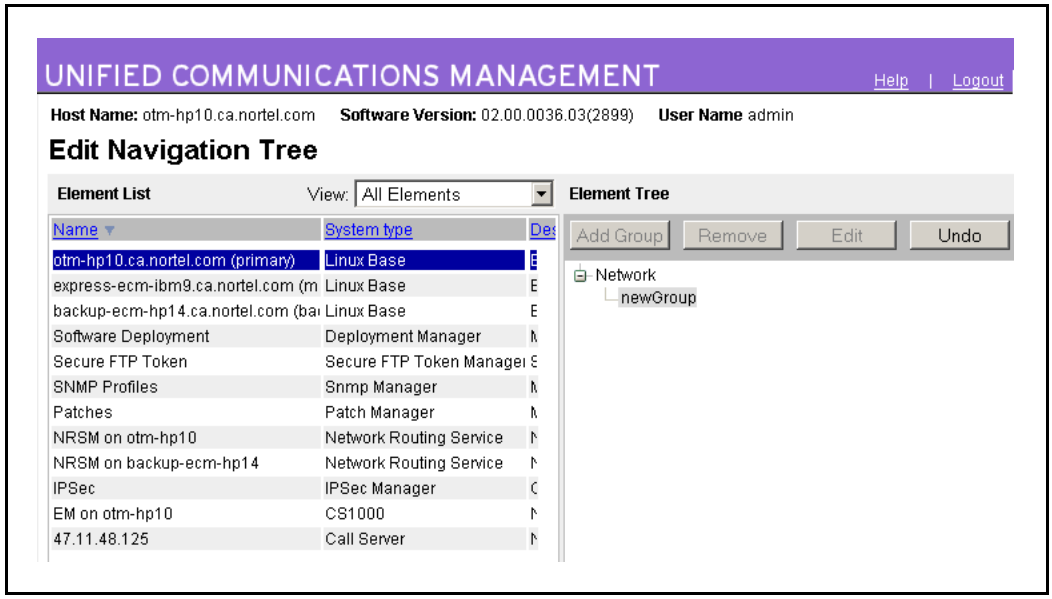
ATTENTION
The Edit Tree button is only visible to authorized administrators.

Adding a group

Use the following procedure to add a new group to the navigation tree.

Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in Figure 34 "Tree view" (page 91).
2	Click **Edit Tree**. The Edit Navigation Tree window appears, as shown in Figure 36 "Edit navigation tree" (page 93).
3	Right-click on the parent in the right Element tree pane.
4	Choose **Add Group** from the shortcut menu. **OR** Select the parent from the right Element tree pane, and click **Add Group**. A New Group window appears. **ATTENTION** The parent of the new group must be a group. Elements cannot contain other groups or elements, but a group can contain both elements and other groups.
5	Complete the following fields: • Type a name for the new group. In the figure Figure 33 "New group" (page 91), the name of the new group is called newGroup. The name can be up to 32 characters. Special characters are allowed. • Type an optional description of the new group. The description can contain up to 500 characters. • Type an optional URL of an element associated with the group. The administrator can navigate to the associated element by clicking the group in navigation mode if the URL is specified. The administrator can also associate a primary cluster element with a group of elements in a cluster when the URL is specified.
6	Click **OK**. The new group appears as the last child of the parent, as shown in the following figure.

Figure 33
New group



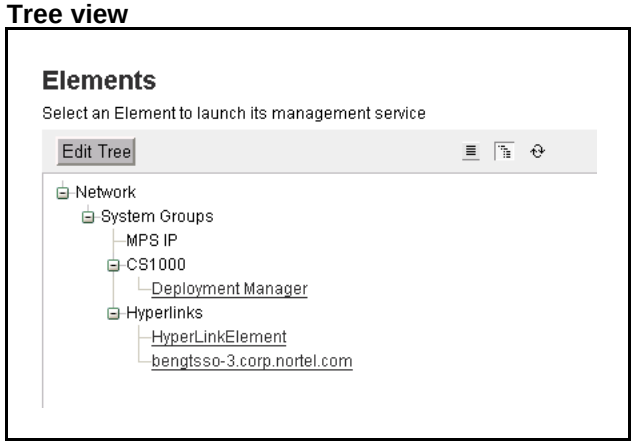
--End--

Adding elements

You cannot add an element to a group in which it already exists. IPsec must be disabled before elements are added to the security domain. Use the following procedures to move an element to a specific position.

Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in the following figure.

Figure 34
Tree view

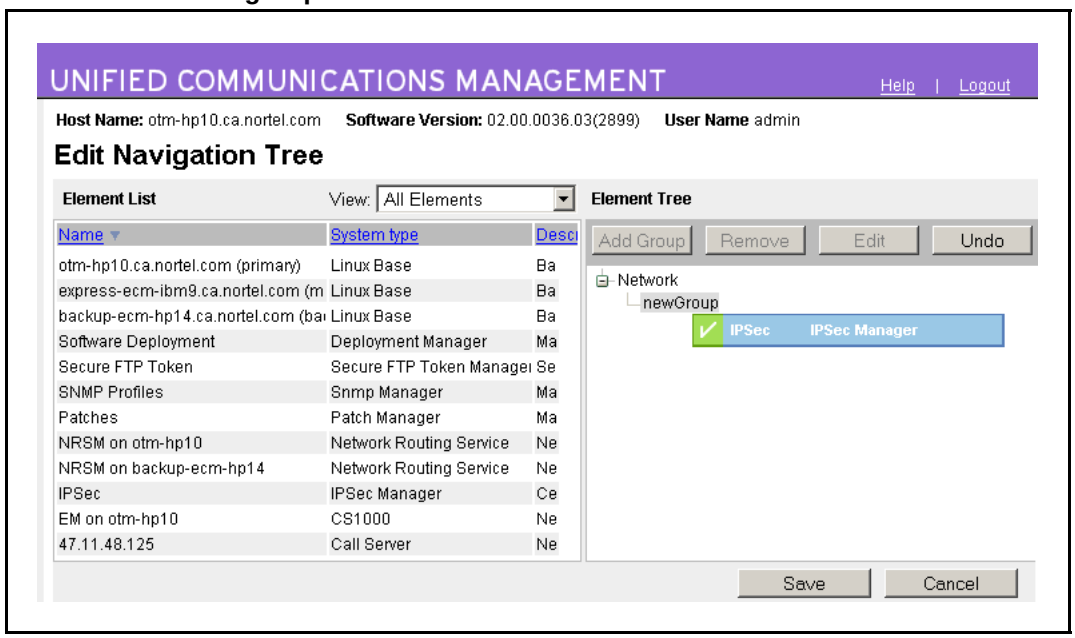


2 Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in Figure 36 "Edit navigation tree" (page 93).

3 Select an element from the Element List in the left pane and drag the element to the destination group in the Element Tree in the right pane. In the following figure, the IPSec element in the left pane is moved to newGroup under the selected parent. The green check mark indicates the IPSec element can be added to the group. If the folder is collapsed, hold the pointer over the group in the Element Tree pane to expand it.

Figure 35
Add elements to a group



ATTENTION

The parent of the new element must be a group. Elements cannot contain other groups or elements. You cannot add an element to a group in which it already exists. Duplicate group name are not permitted under the same parent branch, if the user tries to add an element with a duplicate group name, a pop-up message appears indicating the group name already exists.

When a new item is added to the tree, it appears as the last child of the parent group by default.

4 Click **Save** to add the element to the tree and make this element available to other administrators.

--End--

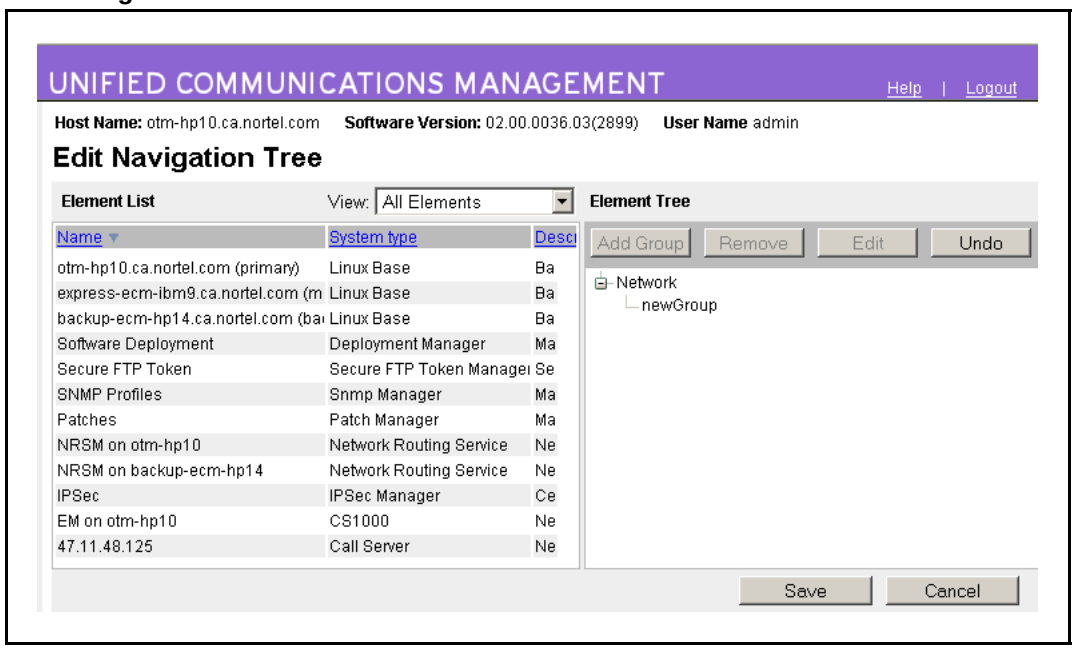
Editing an element

Edit an element using the Edit Navigation Tree.

ATTENTION
The Edit Tree button is only visible to authorized administrators. Edit the tree view using a single logon session. Editing the tree view simultaneously from two or more sessions can cause an inconsistent state to the tree.

Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in Figure 34 "Tree view" (page 91).
2	Click **Edit Tree**. The Edit Navigation Tree window appears, as shown in the following figure.

Figure 36
Edit navigation tree



3	Use the **View** list to show all elements or only the elements not added to the tree. Sort the list by clicking on any column header.
4	Use the Element Tree pane to select the element and click Add Group, Remove, Edit, or Undo. **OR** Right-click a group or element in the Element List pane to invoke a shortcut menu and choose Add Group, Edit, Cut, Copy or Remove.

5 Click **Save** to commit the changes to the element tree and make them available to all administrators.

OR

Click **Cancel** to discard any changes made to the element tree, and exit edit mode.

ATTENTION
Click the Save button to save changes to the tree. If the administrator logs off, navigates away from the page, or a session timeout occurs, the unsaved changes to the tree are lost.

--End--

Editing a group

Edit a group using the Edit Navigation Tree.

ATTENTION
Items in the tree cannot be siblings of a Network group.

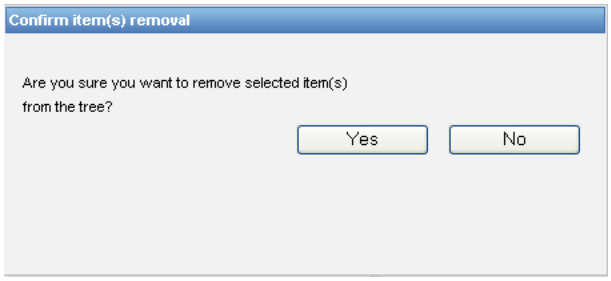
Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in Figure 34 "Tree view" (page 91).
2	Click **Edit Tree**. The Edit Navigation Tree window appears, as shown in Figure 36 "Edit navigation tree" (page 93).
3	Right-click a group in the right pane and choose **Edit** from the shortcut menu or click the **Edit** button. The Rename Group window appears.
4	In the Rename Group window, edit the following fields as required: • Name • Description • URL
5	Click **OK** to accept your changes.
6	Click **Save** to save your changes.

--End--

ATTENTION
You must click Save in the Edit Navigation Tree to save the changes.

Removing items using the Edit Navigation Tree

Remove items using the Edit Navigation Tree.

Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in Figure 34 "Tree view" (page 91).
2	Click **Edit Tree**. The Edit Navigation Tree window appears, as shown in Figure 36 "Edit navigation tree" (page 93).
3	Right-click a group in the right pane, and choose **Remove** from the shortcut menu or click the **Remove** button. A Confirm item(s) removal dialog box appears. **Figure 37** **Confirm item removal dialog box** 
4	Click **Yes** to remove the selected item from the tree.

--End--

ATTENTION
If you remove a group, all children are removed from the tree. Removed elements appear in the Element List in the left pane under Ungrouped Elements, if there are no other instances of them in the tree.

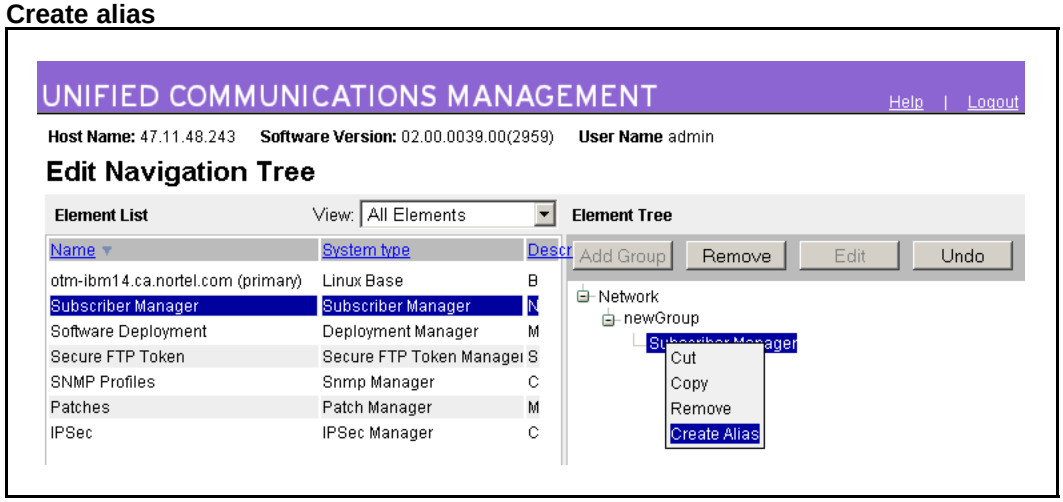
Items are removed from the tree view. To remove the items from Security Services, you must click Save in the Edit Navigation Tree.

Assigning an element alias

The administrator can assign an alias to an element instance to allow for a more descriptive name. Different instances of an element can have different aliases assigned. Aliases appear in an italicized font to indicate an alias in the navigation tree. Move the pointer over an alias element to display element name, type, IP address, and trust status details.

Step	Action
1	On the **Elements** page, click the tree view icon. The tree view appears, as shown in Figure 34 "Tree view" (page 91).
2	Click **Edit Tree**. The Edit Navigation Tree window appears, as shown in Figure 36 "Edit navigation tree" (page 93).
3	Right-click the element and choose **Create Alias** from the shortcut menu as shown in the following figure.

Figure 38
Create alias



Step	Action
4	Type a new name for the element, and press **Enter** to accept the change or **Escape** to cancel renaming the element.
5	Commit the change to the Edit Navigation Tree by clicking **Save**.

--End--

ATTENTION
You cannot assign the same alias to different elements although you can assign aliases to various instances of the same element in the navigation tree. You cannot assign an alias name that is already the name of another element.

Removing an element alias

Remove an element alias.

Step	Action
1	Right-click the element alias.
2	Choose **Remove Alias** from the shortcut menu. The original element name is restored.
3	Commit the change to the Edit Navigation Tree by clicking **Save**.

--End--

Manage elements using table view

Use the procedures in this section to manage elements in UCM common services.

To add a hyperlink type element to UCM, the element must be named and the management address (URL) defined so you can navigate to it. The element must then be incorporated into Security Services by mapping authorization permissions offered by the element to user roles created in UCM. Role permission mapping allows group-based authorization across all elements. Individual user capabilities are limited by the roles to which they are assigned.

For more information about Element permissions, see “Editing user role mapping” (page 116).

Use the following procedures to manage applications using the table view.

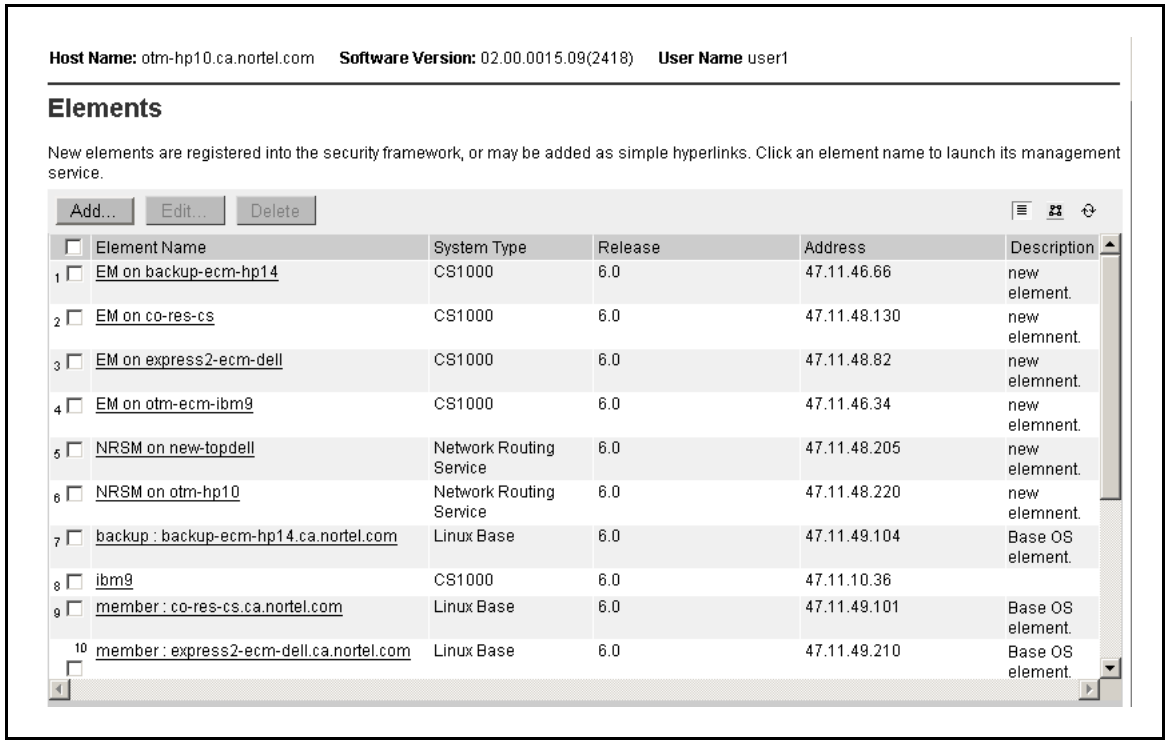
ATTENTION
Your role permissions determine the elements you can see. Network administrators can see all elements.

Starting a managed element

Start the management application for a selected element in the current or a new Web browser.

Step	Action
1	Log on to UCM.
2	In the navigation tree, click **Elements**. The Elements Web page is the default Web page that appears when UCM is opened, as shown in the following figure.

Figure 39
Elements Web page



3 In the **Element Name** column, click an item.

The application for the element appears in the same Web browser window.

To start 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--

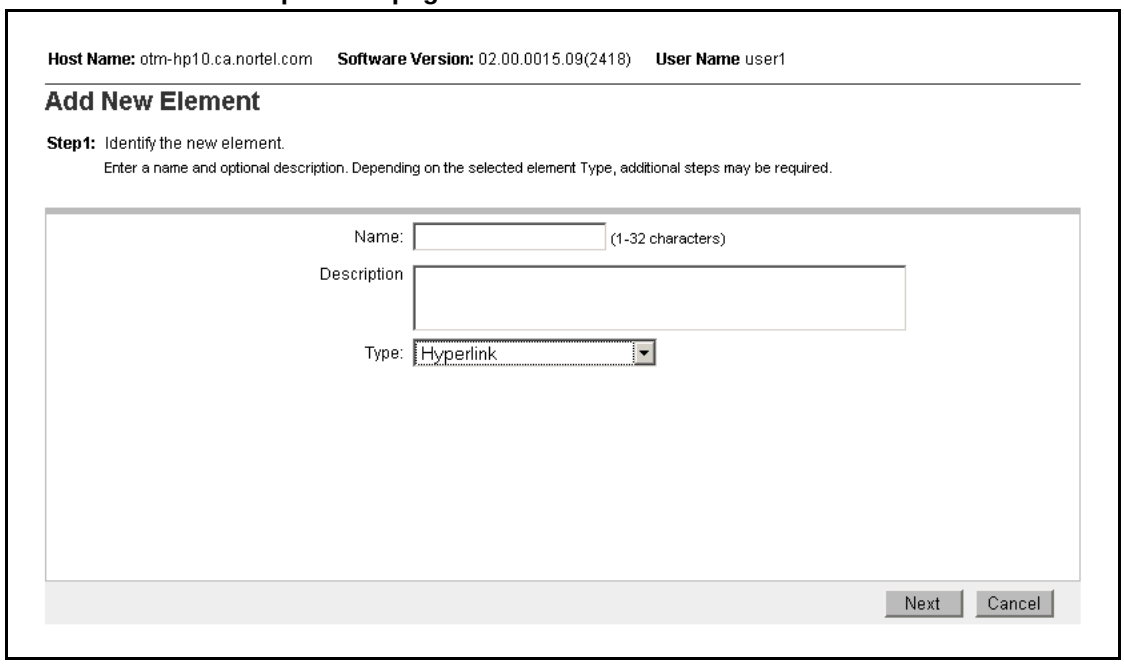
ATTENTION
If the element you attempt to view is a secured element in Security Services, you do not require authentication. If the element is an unsecured element, the administrator is subject to the authentication method because single sign-on is not available for elements outside of UCM .

Adding a Hyperlink

Add an external hyperlink element in UCM.

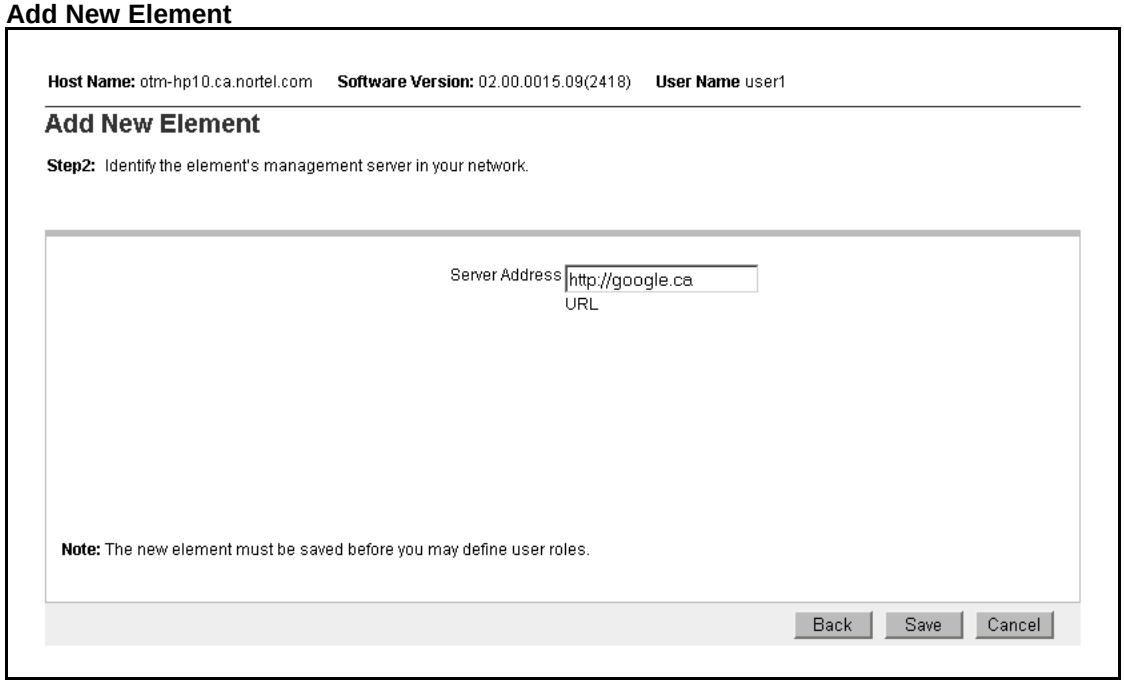
Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Network, Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	Click **Add**. The Add New Element page appears, as shown in the following figure.

Figure 40
Add New Element Step 1 Web page



Step	Action
4	In the **Name** field, type the element name. **ATTENTION** The name must be from 1 to 32 characters. Special characters are permitted.
5	In the optional **Description** field, type a description.
6	Select **Hyperlink** in the **Type** list.
7	Click **Next**. The Add New Element Web page appears for the element, as shown in the following figure.

Figure 41
Add New Element



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

9 Click **Save**.

The Elements Web page appears and the new element appears in the list.

--End--

Adding a CallPilot Messaging element

When Subscriber Manager is deployed, you can add an external CallPilot Messaging element in UCM.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Network**, **Elements**.
3	The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98)
4	Click **Add**. The Add New Element page appears.
5	In the Name field, type the element name. The name must be between 1 to 256 characters in length.
6	In the optional **Description** field, type a description.

7 Select **CallPilot Messaging** in the **Type** list.

8 Click **Next**.

The Add New Element Web page appears for the element.

9 Configure the following CallPilot element management information:

- CallPilot Manager address
- CallPilot server address
- Administrator mailbox number: The Mailbox number to use when communicating with the CallPilot. CallPilot requires the mailbox number to be from 3- to 18-digits in length; however, the element definition does not enforce this restriction.
- Administrator password: The password to use when communicating with the CallPilot. Although CallPilot requires the password to be 4- to 16-digits, the element definition does not enforce this restriction.

10 Click **Save**.

The Elements Web page appears and the new element appears in the list.

--End--

Edit Element properties

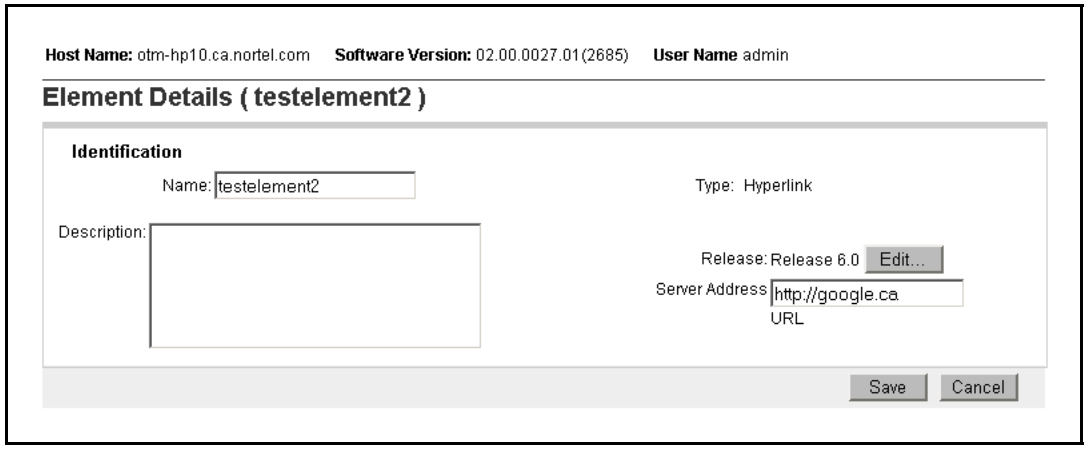
Perform the procedures in this section to edit the properties and role-permission mapping of a hyperlink element, CS 1000 element, Linux base, Network Routing Service or CallPilot Messaging element installed in UCM.

Editing the properties of a hyperlink element

Edit the properties of a hyperlink element in UCM.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	On the Elements Web page, select the check box beside the hyperlink element, and click **Edit**.
4	The Element Details Web page for the selected hyperlink element appears, as shown in the following figure.

Figure 42
Edit Hyperlink properties



5 Modify the following fields:

- Name
- Description
- Release
- Server Address

6 Click **Save**.

--End--

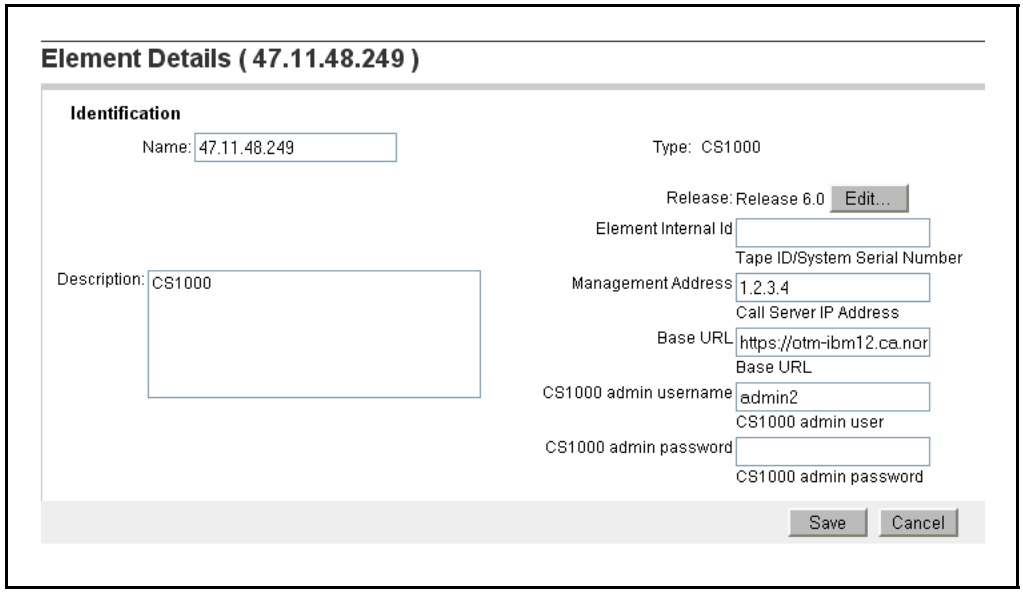
ATTENTION
You cannot modify the element type after you create the element.

Editing the properties for a CS 1000 element

Edit the properties of a CS 1000 element.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	On 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 the following figure.

Figure 43
Element Details Web page



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

- Release
  If the Release is incorrect, click **Edit**.
  The CS 1000 Release Web page appears.
  On the **Release** list, select the desired Release from the available list. Click **Save** to save the changes or click **Cancel** to make no change.
- Name
- Description
- Element Internal Id (Tape ID/System Serial Number)
- Management Address (Call Server IP Address)
- Base URL (where Element Manager is installed)
- CS1000 admin username
- CS1000 admin password
- IPsec Level (select protection level for communication between synchronized targets as Optimized, Functional, or Full)
- Preshared key for configuring IPSec (16–32 characters, do not include "Space ~ * ‘ @ [ ] #)

6 Click **Save**.

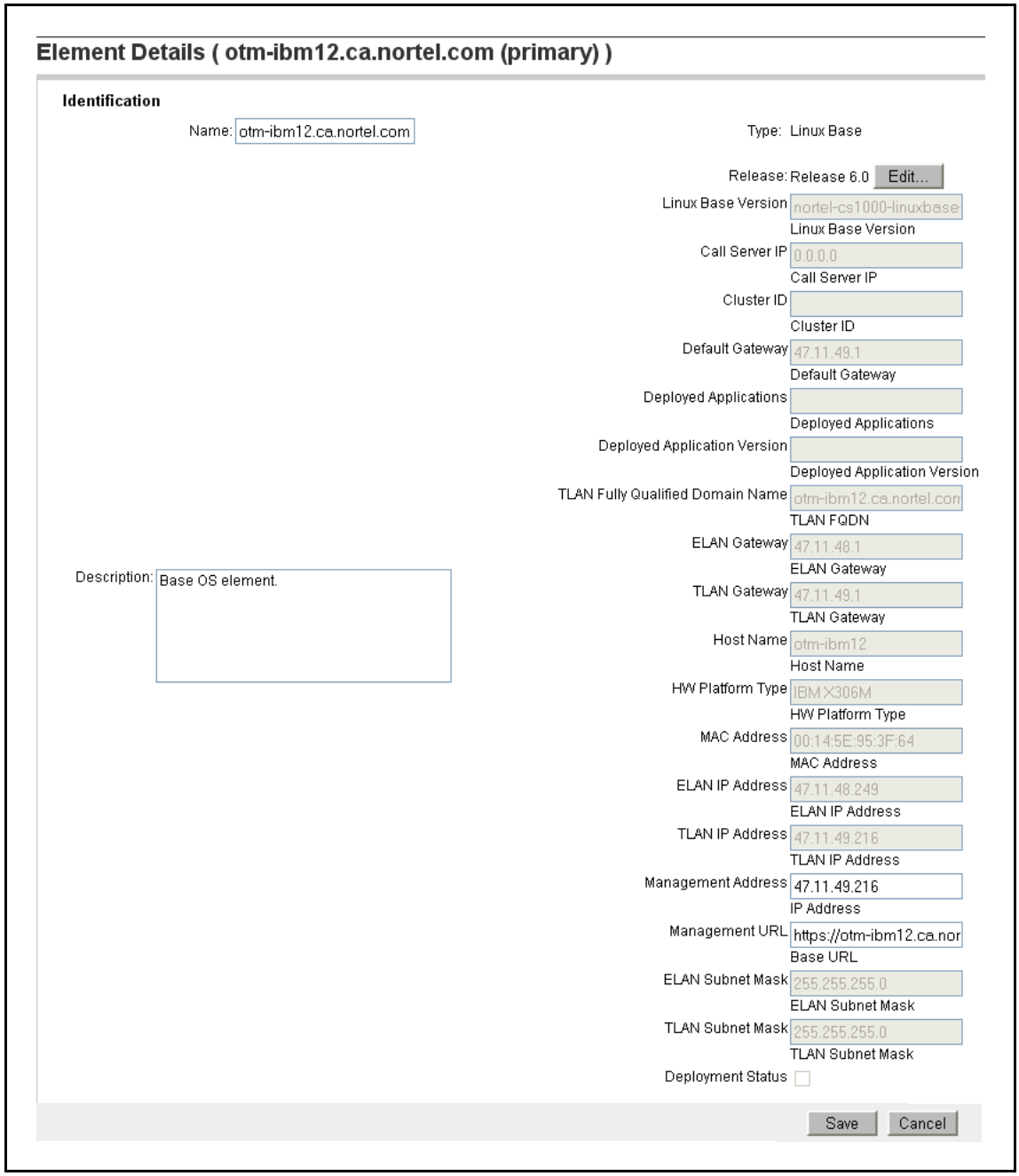
--End--

Editing the properties of a Linux base element

Edit the properties of a Linux base element.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	On the Elements Web page, select the check box beside the Linux base element to edit, and click **Edit**.
4	The Element Details Web page appears, as shown in the following figure.

Figure 44
Element Details Web page



5 Modify the following fields:

- Name
- Description
- Release
- Linux Base Version (read only)

- Call Server IP (read only)
- Cluster ID (read only)
- Default Gateway (read only)
- Deployed Applications (read only)
- Deployed Application Version (read only)
- TLAN Fully Qualified Domain (read only)
- ELAN Gateway (read only)
- TLAN Gateway (read only)
- Host Name (read only)
- HW Platform Type (read only)
- MAC Address (read only)
- ELAN IP Address (read only)
- TLAN IP Address (read only)
- Management Address (IP address)
- Management URL (Base URL)
- ELAN Subnet Mask (read only)
- TLAN Subnet Mask (read only)
- Deployment Status

6 Click **Save**.

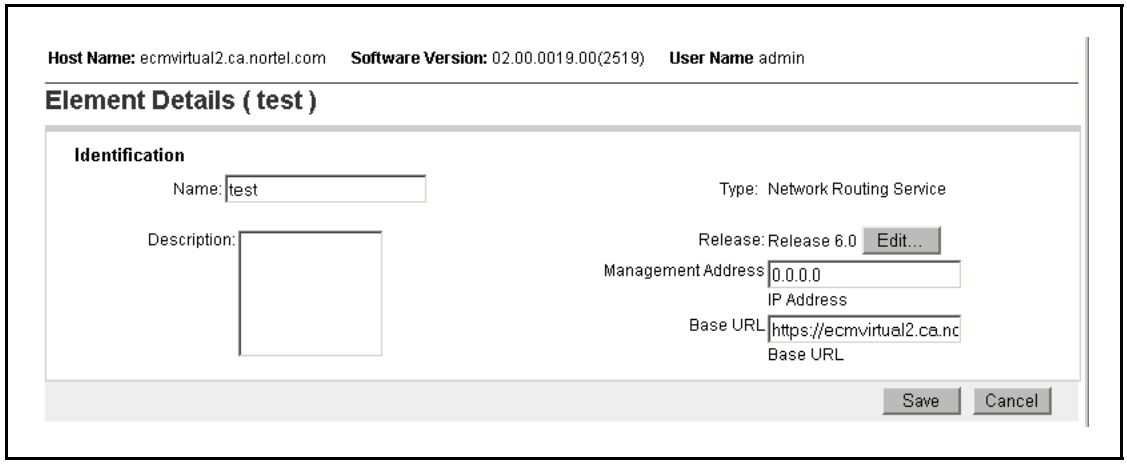
--End--

Editing the properties of a Network Routing Service element

Edit the properties of a Network Routing Service element.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	On 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 the following figure.

Figure 45
Element Details Web page for a Network Routing Service element



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

- **Name**
- **Description**
- **Release**
- **Management Address**
- **Base URL** (where NRS Manager is installed)

6 Click **Save** .

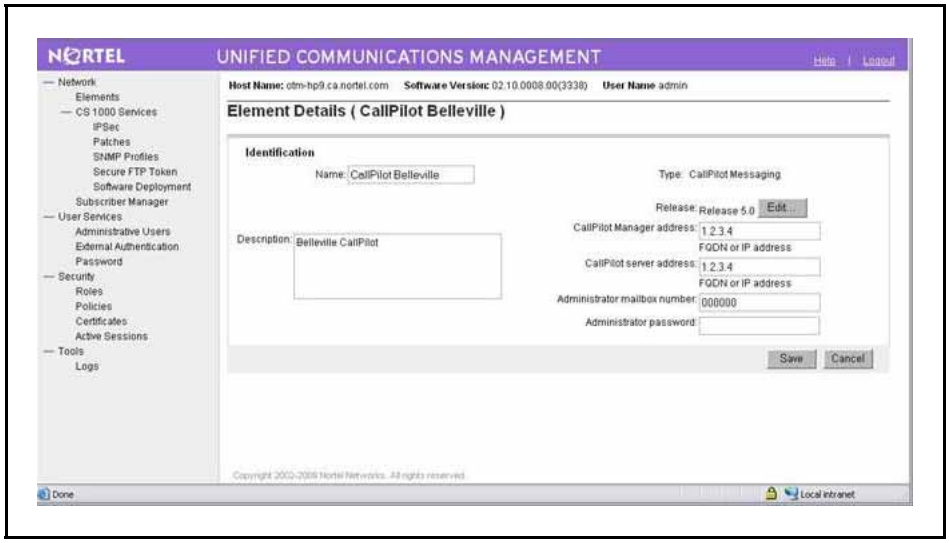
--End--

Editing the properties of a CallPilot Messaging element

Edit the properties of a CallPilot Messaging element in UCM.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in the following figure.

Figure 46
Element Details Web page



3 In the **Identification** section, edit the following fields as required:

- **Name**
- **Description**
- **Release**
- **CallPilot Manager address**
- **CallPilot server address**
- **Administrator mailbox number**
- **Administrator password**

4 Click **Save**.

ATTENTION
You cannot modify the element type after you create the element.

--End--

Deleting selected elements

Delete elements that are no longer required.

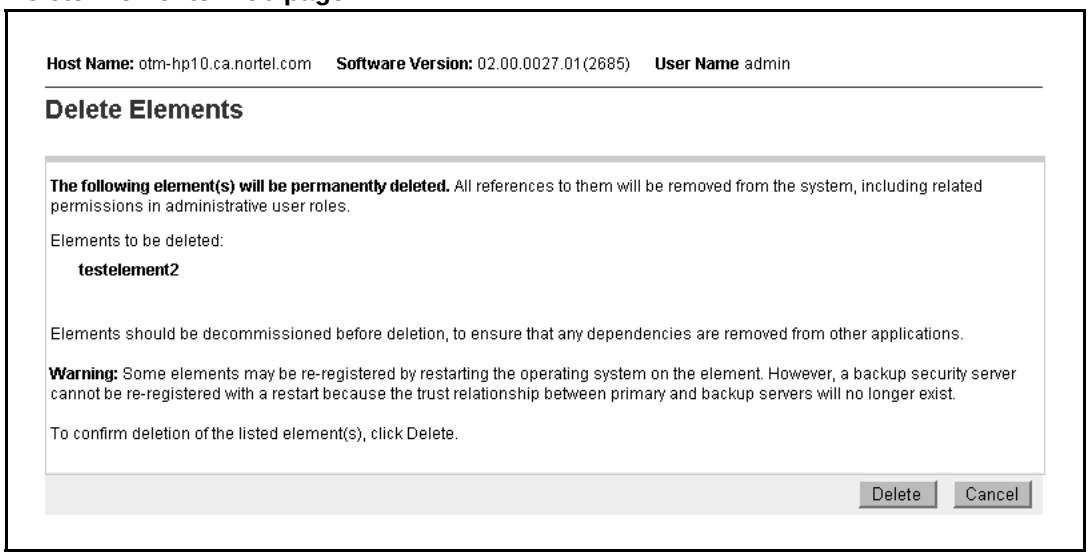
ATTENTION
If the backup security server is deleted, the trust between the primary and backup server is broken and the backup server cannot function as a backup server in the security domain. If the Linux base element from the elements table is removed, it reregisters but is not physically removed. Click the Refresh link on the Elements page if you cannot add new elements or delete selected elements after the security service is restarted.

Prerequisites

Elements must be physically decommissioned prior to deleting the element from the elements table.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 39 "Elements Web page" (page 98).
3	On the Elements Web page, select the check box beside one or more elements. **ATTENTION** The Primary security server element cannot be deleted from the element table. Any attempt to delete the primary server is blocked in UCM.
4	Click **Delete**. The Delete Elements Web page appears, as shown in the following figure.

Figure 47
Delete Elements Web page



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

--End--

ATTENTION
You can access management applications of a deleted element. UCM maintains an in-memory cache for all elements accessed from the current Web server. When a user deletes an element, the in-memory cache contains the information for the element; however, all permissions on an element are denied after the user deletes the element.

CS 1000 Services

This section contains information about configuring servers on the Communication Server 1000 including patching, IP Security, and SNMP.

IPsec

Use IPsec for network-wide policy implementation and synchronization of preshared keys across network targets. IPsec is included as part of the UCM installation and is configured on the Primary Security server.

In the Network branch of the UCM navigation tree, click CS 1000 Services, IPsec. You can administer several aspects of IP security, such as configuring domain-wide security policy, adding and removing of IPsec targets, enabling or disabling of IPsec for network elements, and scheduling of IPsec synchronization and activation. For more information about using IPsec, see *Security Management Fundamentals* (NN43001-604.)

Patches

In the Network branch of the UCM navigation tree, click CS 1000 Services, Patches. Use Patching Manager on the primary security server to remotely deploy patches from a central location to other Linux servers on the same security domain. The Patching Manager screen appears with a list of all Linux servers (or Linux Base Elements) in the same security domain.

You can also install patches locally. Local Patching is accessible from the Base Manager of each Linux Element. Patching Manager can be reached by logging on to the primary security server and clicking an element or by logging on locally to the element. For more information about Patching Manager, see *Patching Fundamentals* (NN43001-407).

SNMP Profiles

In the Network branch of the UCM navigation tree, click CS 1000 Services, SNMP Profiles. You can add an SNMP profile, configure an existing SNMP profile, and delete an SNMP profile. For more information about SNMP profiles, see “SNMP Profiles” (page 24).

For more information about configuring SNMP Profiles, see Communication Server 1000 Fault Management — SNMP (NN43001-719).

Secure FTP token

In the Network branch of the UCM navigation tree, click CS 1000 Services, Secure FTP Token. The Secure FTP Token Management screen appears on which you can view the date of the last generated token, refresh the status of the current token, and regenerate a new token for distribution throughout the network. For more information about Secure FTP Token, see *Security Management Fundamentals* (NN43001-604).

Software Deployment

In the Network branch of the UCM navigation tree, click Software Deployment. Use Software Deployment on the primary security server to remotely deploy application software from a central location to other Linux servers in the same security domain.

On the Deployment Manager Web page, you can select the following items:

- Deployment
- Software Loads
- Backups
-

You can also deploy software locally prior to the server joining the security domain; however, Nortel recommends using the central deployment method.

For more information about Software Deployment, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

UCM User Services configuration

This chapter describes the features found in the Unified Communications Management (UCM) navigation pane under the User Services branch.

Navigation

Administrative Users

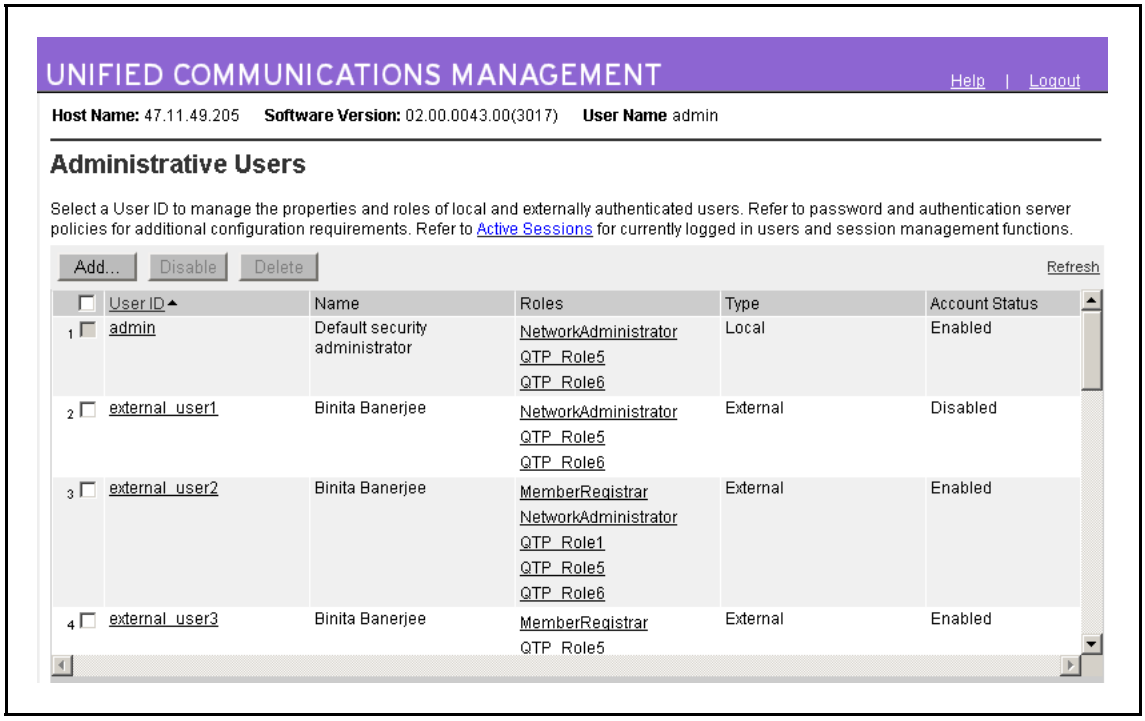
In the User Services branch of the UCM navigation tree, click Administrative Users. The Administrative Users Web page appears. Administrators with the NetworkAdministrator role can perform the user management tasks required to manage users within UCM.

Reviewing existing users

View the users that are configured for UCM access.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page lists users configured for access to UCM. The User ID, Name, Roles, Type, and Account Status are displayed, as shown in the following figure.

Figure 48
Administrative Users Web page



3 Review the information for existing users.

--End--

ATTENTION
The check box for the admin user ID appears dimmed. The admin user ID cannot be changed.

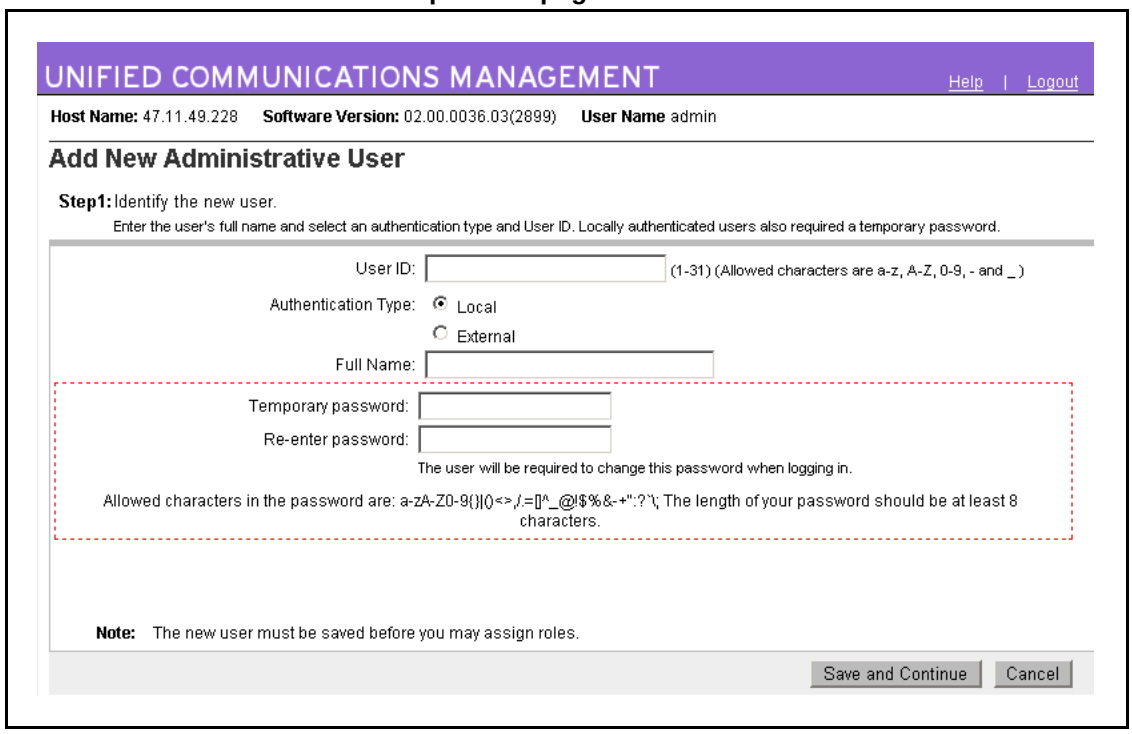
Adding a new local or external user

Use the following procedures to create a new user of UCM and to assign roles to the new user. For more information about local and external users, see “Authentication” (page 43).

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).
3	Click **Add**.

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

Figure 49
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 In the **Authentication Type**, select **Local** or **External**. For more information about local and external users, see "Authentication" (page 43)

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

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

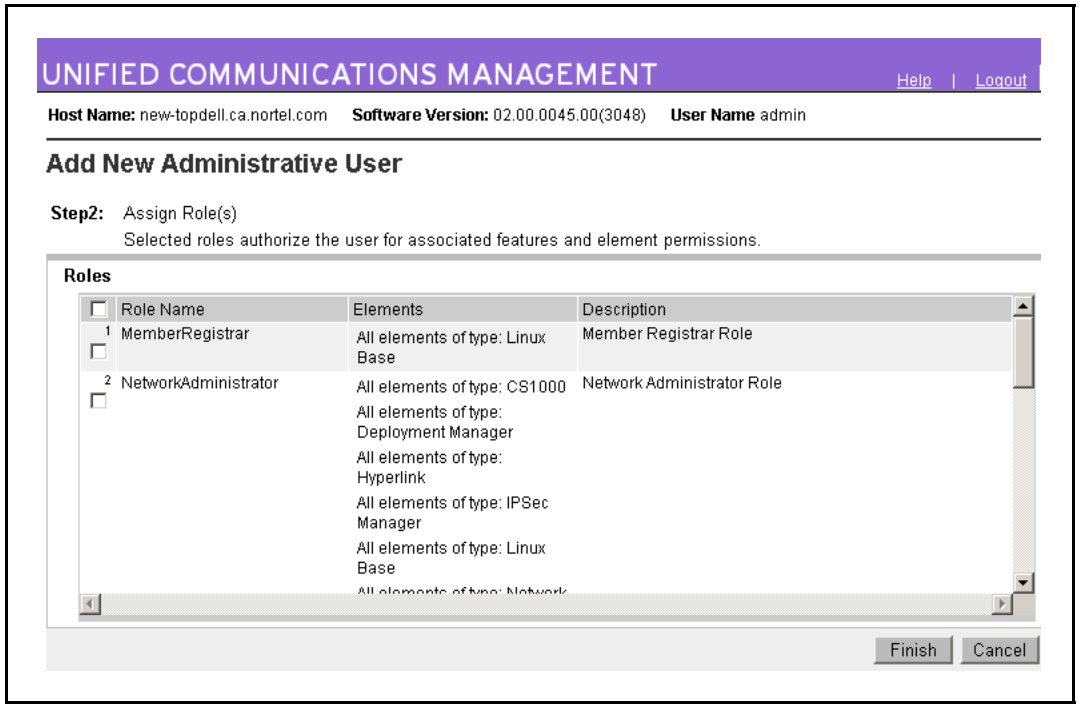
8 In the **Re-enter password** field, type the new password.

ATTENTION
The password that is entered for the new local user is temporary. For the first time logon to UCM, the user is prompted to change the password.

9 Click **Save and Continue**.

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

Figure 50
Add New Administrative User Step 2 Web page



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

11 Click **Finish**.

The Administrative Users Web page appears.

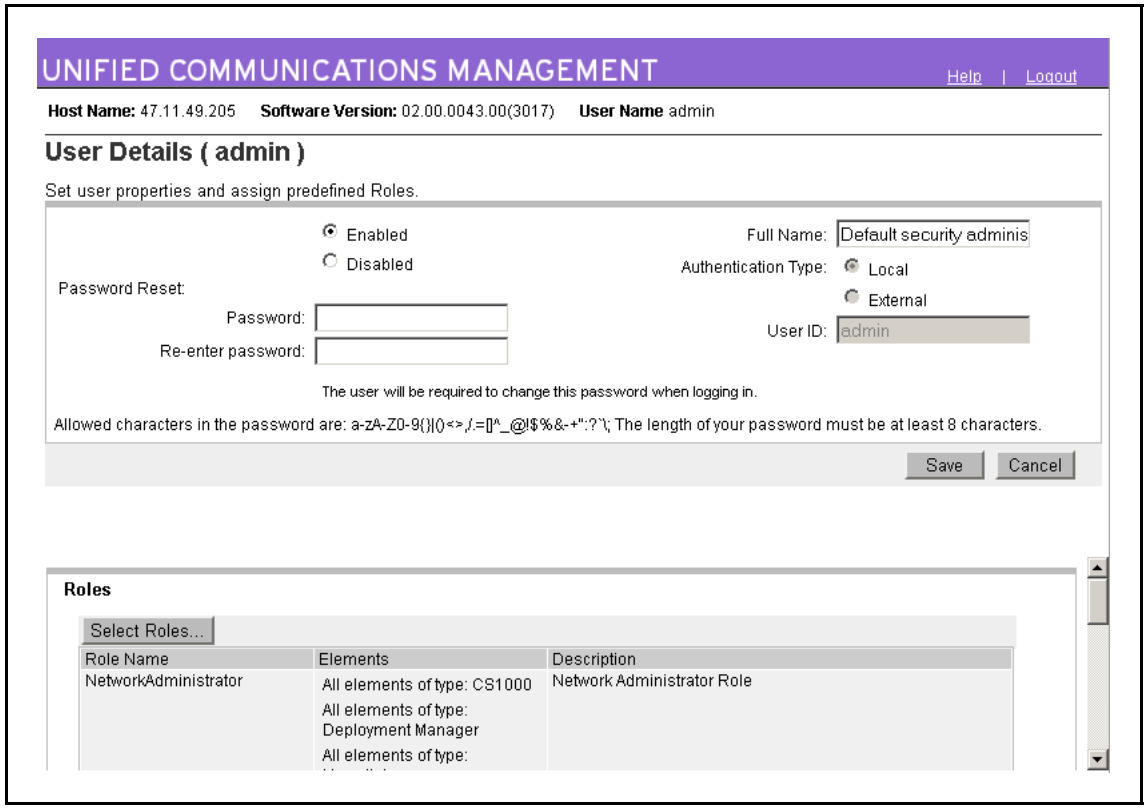
--End--

Editing user role mapping

Select roles to authorize a user for associated features and element permissions.

Step	Action
1	Log on to UCM as an administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).
3	Click the User ID to edit role mapping. The User Details Web page appears, as shown in the following figure.

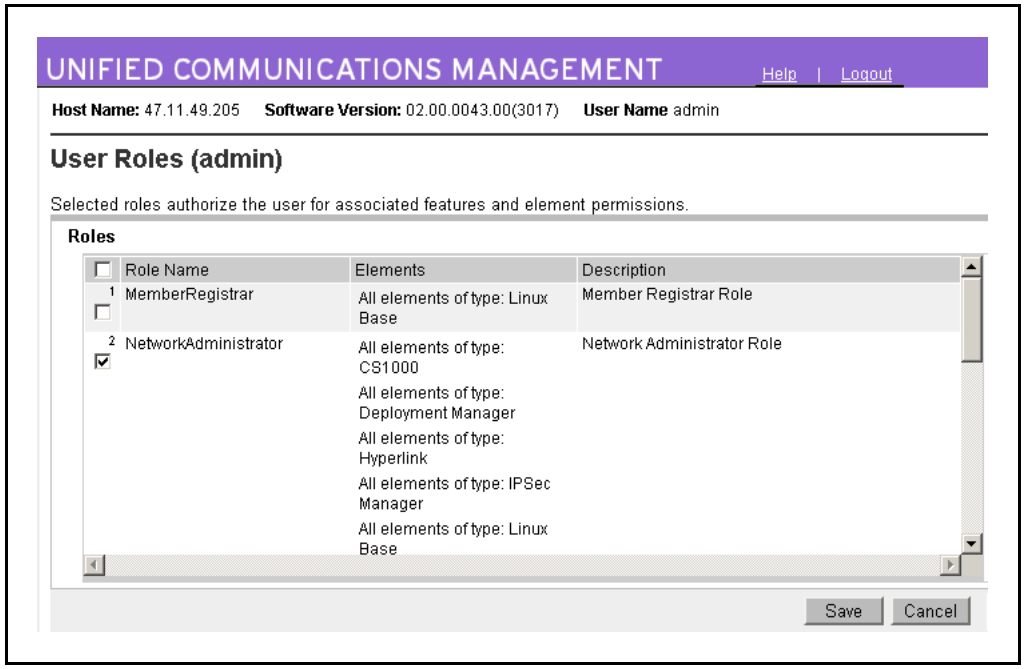
Figure 51
User Details Web page



4 Click **Select Roles**.

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

Figure 52
User Roles Web page



5 Select or clear the roles for the selected user.

6 Click **Save**.

The **User Details** Web page appears, as shown in Figure 51 "User Details Web page" (page 117).

7 Click **Save**.

--End--

Configure the properties of a local user

An administrator with NetworkAdministrator role permission assignment can edit the full name and reset the password for local and built-in administrators. An administrator can also enable or disable accounts and edit the selected administrator's role assignment.

The administrator can change the password and full name for a local user, to disable and enable a local user account, and to delete a user.

Editing 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.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).
3	Click the User ID to edit the password and full name. The **User Details** Web page appears, as shown in Figure 51 "User Details Web page" (page 117).
4	In the **Full Name** field, edit the name of the user.
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:*** For the first time logon, the user is prompted to change the password.
7	Click **Save**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).

--End--

Disabling a user account

Disable one or more user accounts in UCM.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).
3	Click the User ID item. The User Details Web page appears, as shown in Figure 51 "User Details Web page" (page 117)
4	Select the **Disabled** option, and click **Save**. **OR**

5 Select the check box beside the User ID of one or more user accounts as shown in Figure 48 "Administrative Users Web page" (page 114)and click **Disable**.

Log on as the selected user to verify the change.

A user can disable built-in accounts; however, the UCM Security Services does not notify the Linux servers when this occurs. The built-in accounts remain valid in the Linux host account database.

--End--

Enabling a user account

Enable one or more user accounts in UCM.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).
3	Click the User ID for the disabled user account. The User Details Web page appears, as shown in Figure 51 "User Details Web page" (page 117).
4	In the **User Details** Web page, select **Enabled**.
5	Click **Save**.

--End--

Deleting a user account

Delete one or more user accounts in UCM.

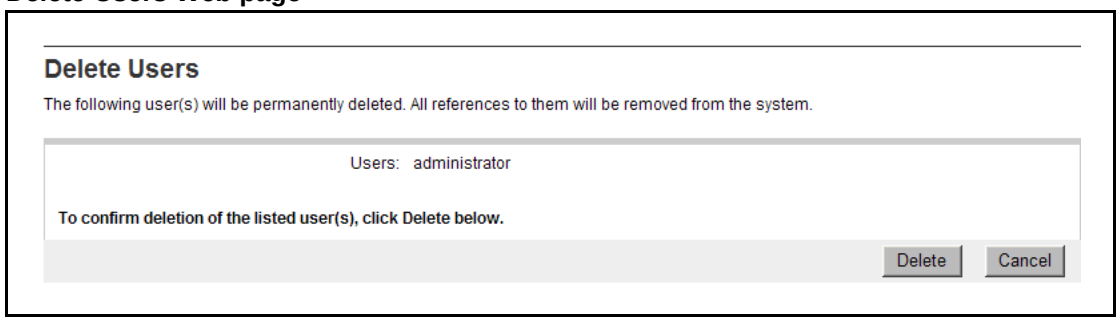
Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **User Services**, **Administrative Users**. The Administrative Users Web page appears, as shown in Figure 48 "Administrative Users Web page" (page 114).

3 Select the check box beside the User ID of one or more user accounts.

4 Click **Delete**.

The Delete Users Web page appears, as shown in the following figure.

Figure 53
Delete Users Web page



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

ATTENTION
Users cannot delete their own accounts.

--End--

External Authentication

In the User Services branch of the UCM navigation tree, click External Authentication. The External Identity Repositories Web page contains a summary page for Authentication scheme and Authentication Servers. You can configure the authentication scheme and the authentication servers for UCM.

UCM 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 order is 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.
- external KERBEROS server

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

You can edit the authentication scheme, as shown in “Editing the authentication scheme” (page 122) and configure the authentication servers as shown in “Provision the authentication servers” (page 123).

Authentication scheme policy

UCM supports up to three authentication authorities:

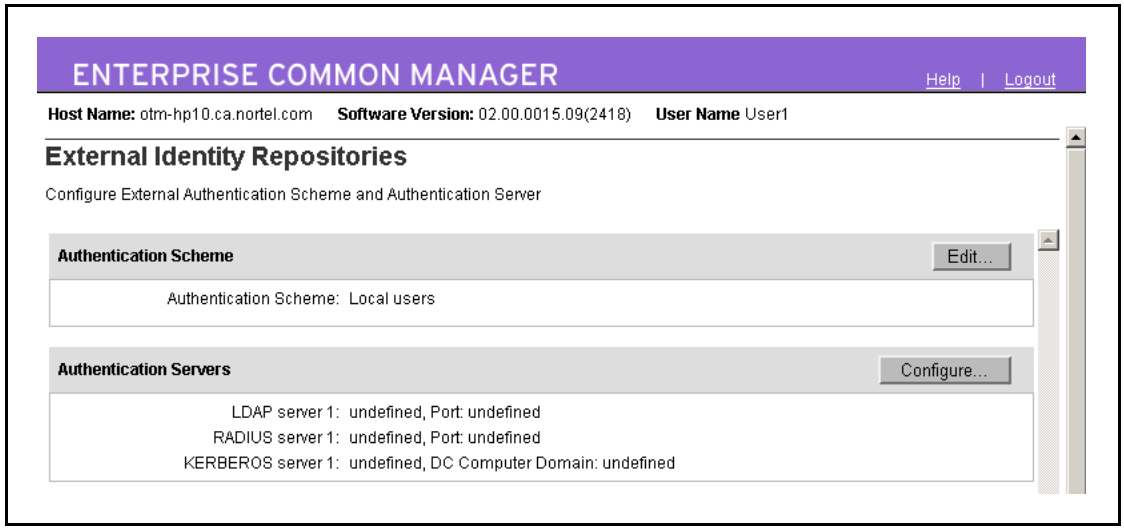
- local servers
- external RADIUS servers
- external LDAP servers (including Sun ONE or Microsoft active directory server)
- Kerberos server

Editing the authentication scheme

Use the following procedure to edit the authentication scheme.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **User Services**, **External Authentication**. The External Identity Repositories page appears, as shown in the following figure.

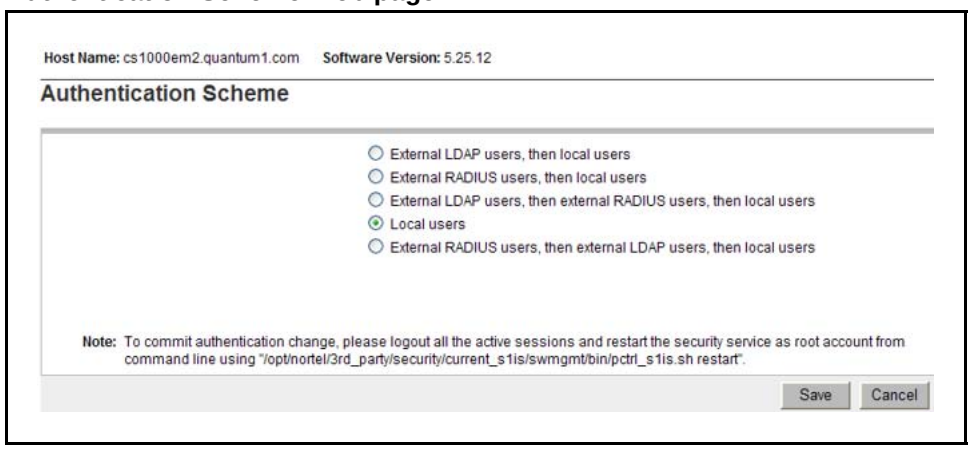
Figure 54
External Identity Repositories



3 In the Authentication Scheme section, click **Edit**.

The Authentication Scheme Web page appears, as shown in the following figure.

Figure 55
Authentication Scheme Web page



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

--End--

Provision the authentication servers

When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the cn attribute of the external users the same as the logon name.

The TCP port used for the external LDAP server and the 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.

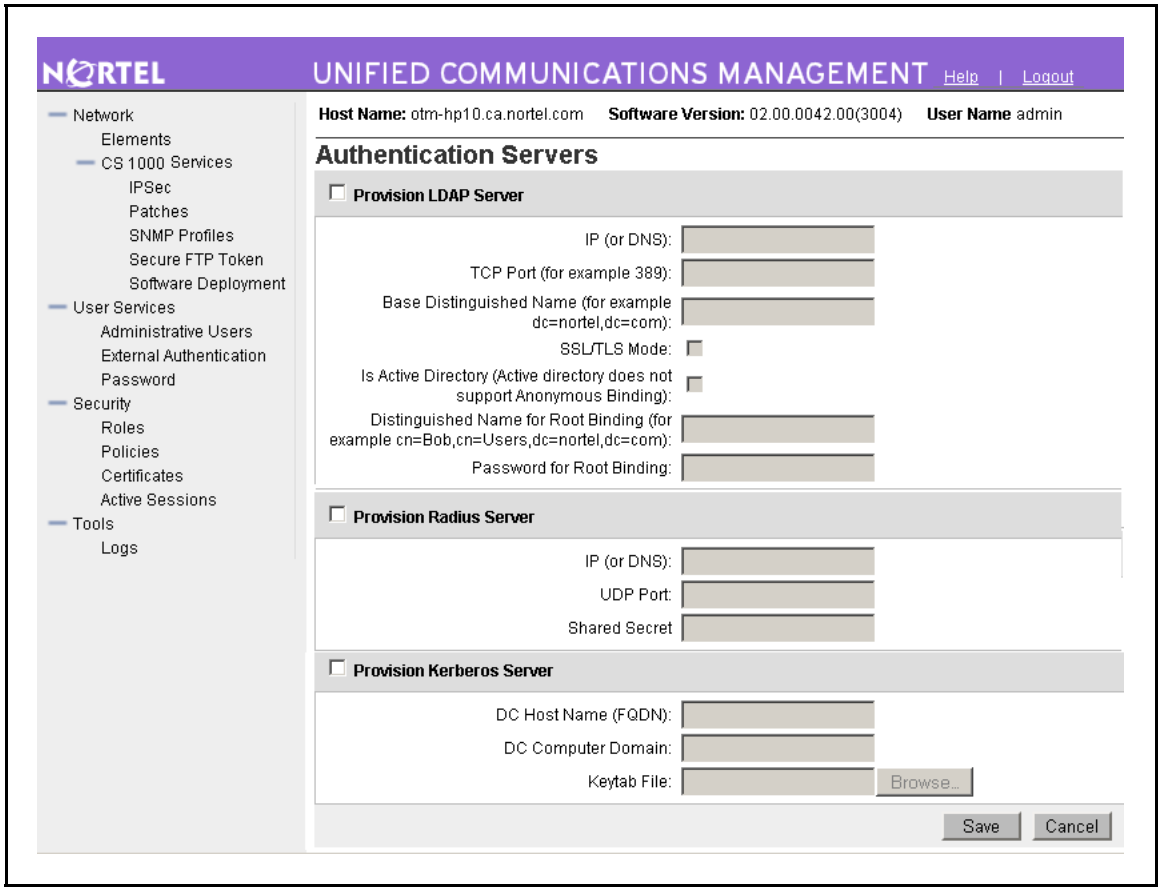
In the Authentication Servers page, you can provision an LDAP, a Radius, or a Kerberos Server, as shown in Figure 56 "Authentication Servers Web page" (page 125).

Provisioning the LDAP Server

Configure the required information for the LDAP authentication server.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **User Services**, **External Authentication**. The External Identity Repositories page appears, as shown in Figure 54 "External Identity Repositories" (page 123).
3	In the Authentication Servers section, click **Configure**. The Authentication Servers Web page appears, as shown in the following figure.

Figure 56
Authentication Servers Web page



4 In the Provision LDAP Server section, complete the following information:

- **IP (or DNS):** Type the IP address or DNS name of the LDAP server.
- **TCP Port:** Type the TC port number of the LDAP server.
- **Base Distinguished Name:** 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 for Root Binding** field, type the password for the root binding.

5 Click **Save**.

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

--End--

Provisioning the Radius Server

Configure the required information for the RADIUS authentication server.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **User Services**, **External Authentication** , as shown in Figure 54 "External Identity Repositories" (page 123). The External Identity Repositories page appears.
3	In the Authentication Servers section, click **Configure**. The Authentication Servers Web page appears, as shown in Figure 56 "Authentication Servers Web page" (page 125).
4	In the Provision RADIUS Server section, complete the following information: • **IP (or DNS):** Type the IP address or DNS name of the primary RADIUS server. • **UDP Port:** Type the UDP port number of the primary RADIUS server. • **Shared Secret:** Type the shared secret of the RADIUS server. **ATTENTION** You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.
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--

Provisioning the Kerberos Server

Configure the required information for the Kerberos server.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **User Services**, **External Authentication**, as shown in Figure 54 "External Identity Repositories" (page 123). The External Identity Repositories page appears.
3	In the Authentication Servers section, click **Configure**. The Authentication Servers Web page appears, as shown in Figure 56 "Authentication Servers Web page" (page 125).
4	In the Provision Kerberos Server section, complete the following information: • **DC Host Name (FQDN):** Type your FQDN in the following format: machineName.domainName.com/net/ • **DC Computer Domain:** Type the domain name of the Kerberos server. • **Keytab File:** Type the encrypted Kerberos server key.
5	Click **Save**.
	--End--

ATTENTION
When logged on to the Kerberos server using Single Sign-on (SSO), you cannot exit from UCM using the Logout link because in this context, SSO automatically authenticates you inside the Domain Controller (DC) domain. You must manually close the browser to exit the application.

Password

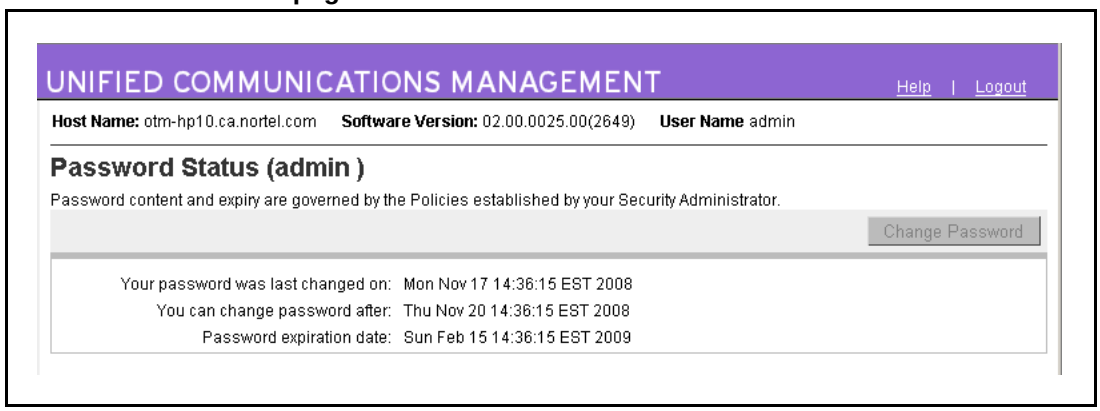
In the User Services branch of the UCM navigation tree, click Password. The Password Status Web page appears. From the Password Status Web page, users can view the status for a local account password and change a local account password.

Reviewing the status of a local account password

Determine when a local password can change and when the password expires.

Step	Action
1	Log on to the UCM common services.
2	In the navigation tree, click **User Services**, **Password**. The Password Status Web page appears, as shown in the following figure.

Figure 57
Password Status Web page



ATTENTION
An external user cannot review or change the password.

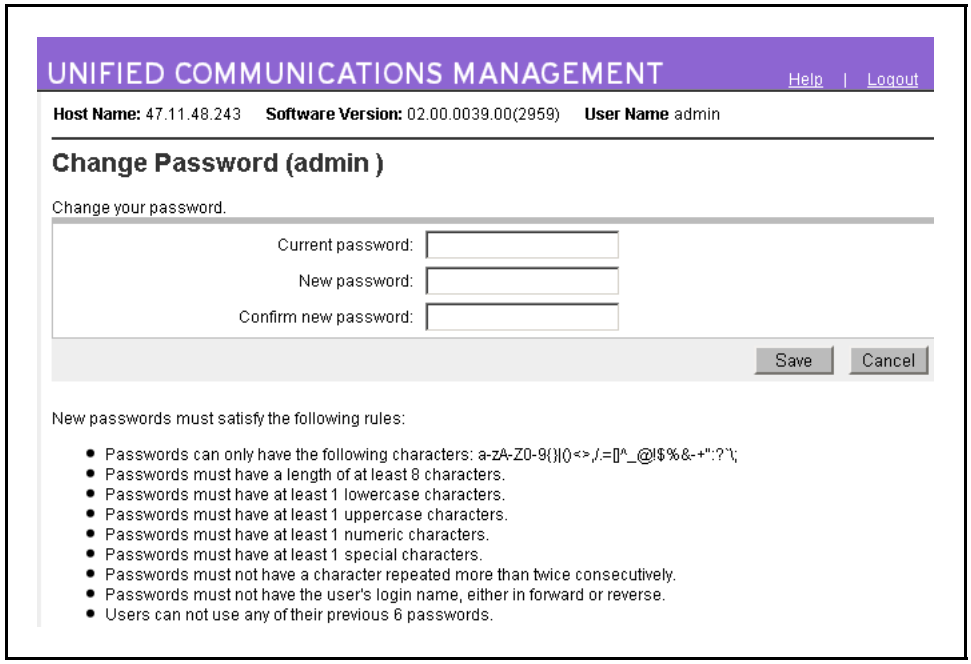
--End--

Changing a local account password

Change the current password.

Step	Action
1	Log on to UCM Common Services.
2	In the navigation tree, click **User Services**, **Password**. The Password Status Web page appears, as shown in Figure 57 "Password Status Web page" (page 128).
3	Click **Change Password**. The Change Password Web page appears, as shown in the following figure.

Figure 58
Change Password Web page



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

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

ATTENTION
The default password strength policy is defined by your network administrator. Follow the password strength policy requirements shown on the Change Password Web page.

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

7 Click **Save**.

--End--

UCM Security configuration

This chapter describes the security features found in the Unified Communications Management (UCM) navigation pane under the Security branch.

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

- Roles: manage users and roles
- Policies: manage password policies, single sign-on cookie domain, and logon warning banner
- Certificates: manage certificates
- Active Sessions: view and terminate active sessions

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

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

Navigation

Roles

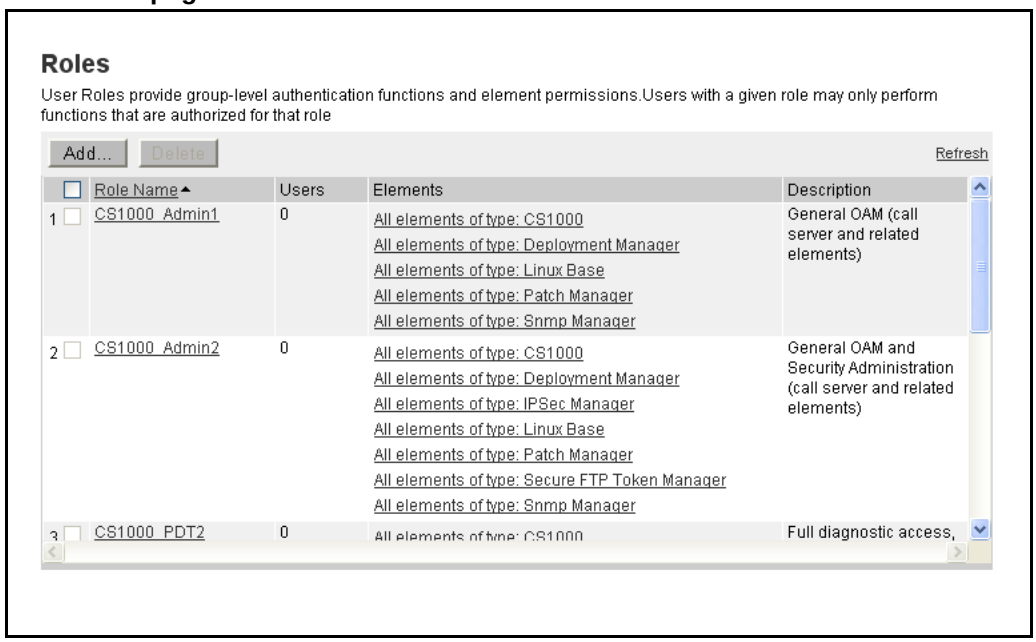
In the Security branch of the UCM navigation tree, click Roles. The Roles Web page appears. From the Roles Web page, network administrators can perform the various role management tasks required to manage roles within UCM.

In UCM, users must be given permissions to perform tasks. UCM Security Services supports two types of roles–built-in and custom roles. The built-in roles that can be assigned to users are MemberRegistrar, NetworkAdministrator, Patcher, CS1000_Admin1, CS1000_Admin2, CS1000_CLI_REGISTRAR and CS1000_PDT2, as shown in Figure 59 "Roles Web page" (page 132). Within these roles, you have access to various elements and from there you can choose specific permission mappings. The built-in roles in UCM are not editable. For more information about built-in roles, see “Built-in roles” (page 50).

For more information about creating custom roles, see “Adding a custom role” (page 133).

ATTENTION
If an administrator has multiple roles assigned, the permission is granted based on the highest privileged algorithm.

Figure 59
Roles Web page



Reviewing existing roles

View the current roles in UCM.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **Security**, **Roles**.

The Roles Web page appears with a list of available roles, as shown in Figure 59 "Roles Web page" (page 132).

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

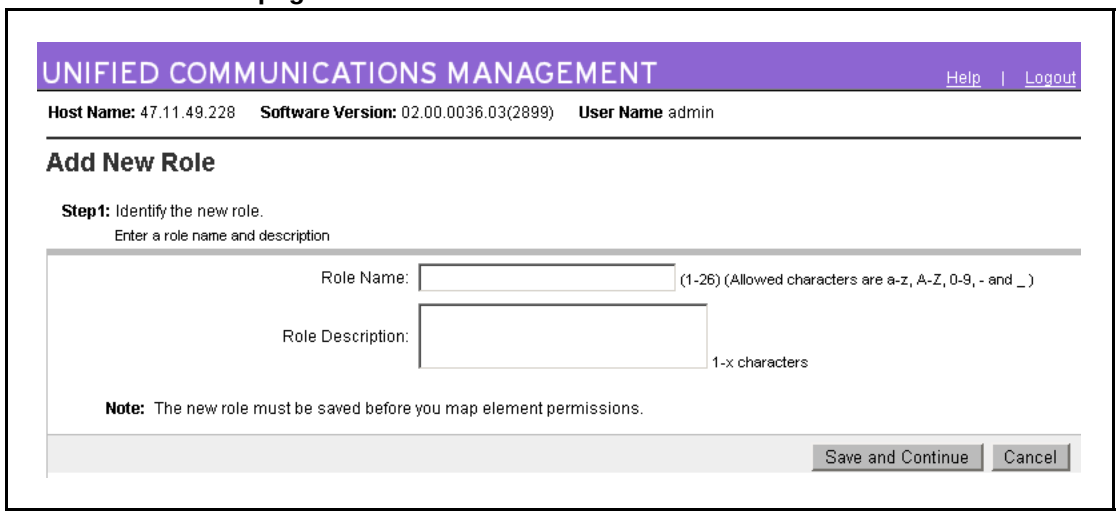
--End--

Adding a custom role

A network administrator can add custom roles to map to specific elements, for example a single CS 1000 element, and then customize permissions for that element.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **Security**, **Roles**.
	The Roles Web page appears with a list of available roles, as shown in Figure 59 "Roles Web page" (page 132).
3	Click **Add**.
	The Add New Role Web page appears, as shown in the following figure.

Figure 60
Add New Role Web page



Note: The role name must be from 1 to 26 characters in length. Allowed characters are a-z, A-Z, 0-9, - and _

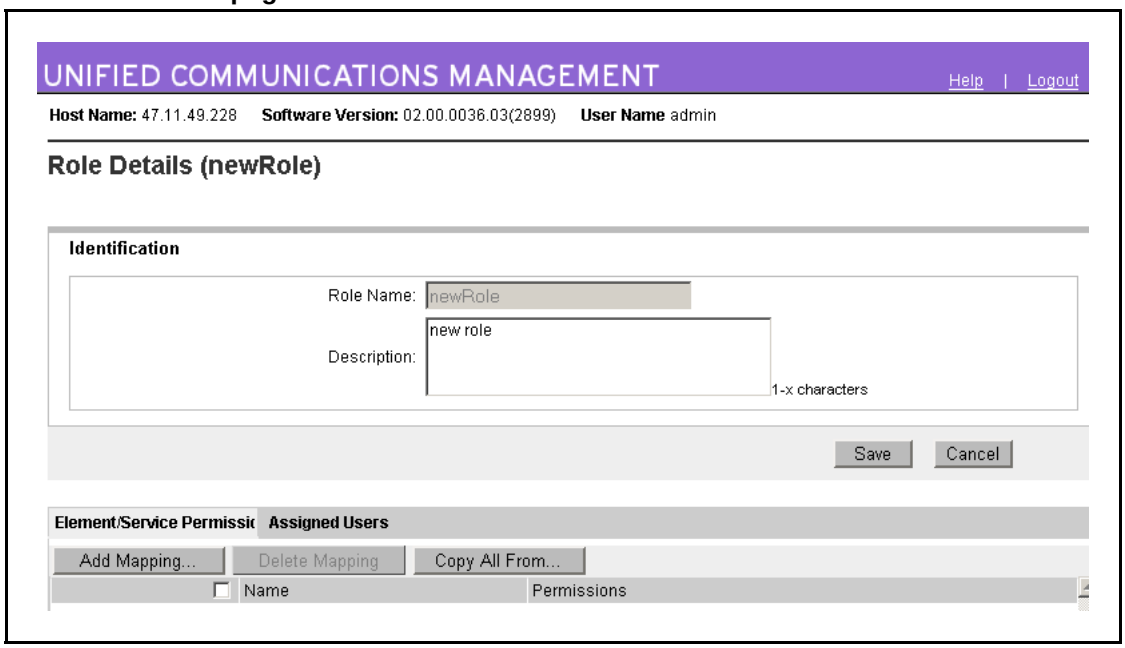
4 In the **Role Name** field, type the unique role name.

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

6 Click **Save and Continue**.

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

Figure 61
Role Details Web page

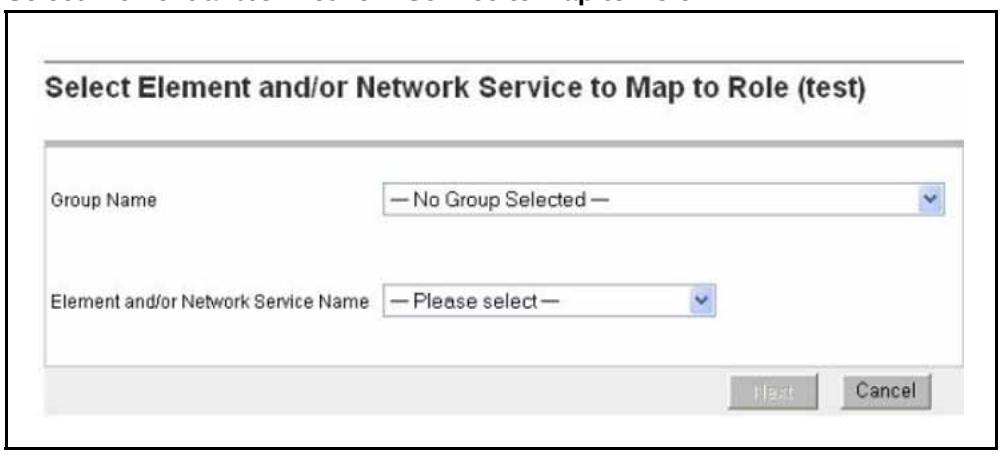


7 Click the **Element/Service Permission mapping** tab.

8 Click **Add Mapping**.

The Select Element and/or Network Service to Map to Role (newRole) page appears, as shown in the following figure.

Figure 62
Select Element and/or Network Service to Map to Role



9 Select a Group Name (optional) and an element to map to a role. You can select an element by individual element name or an element by type. Click **Next.**

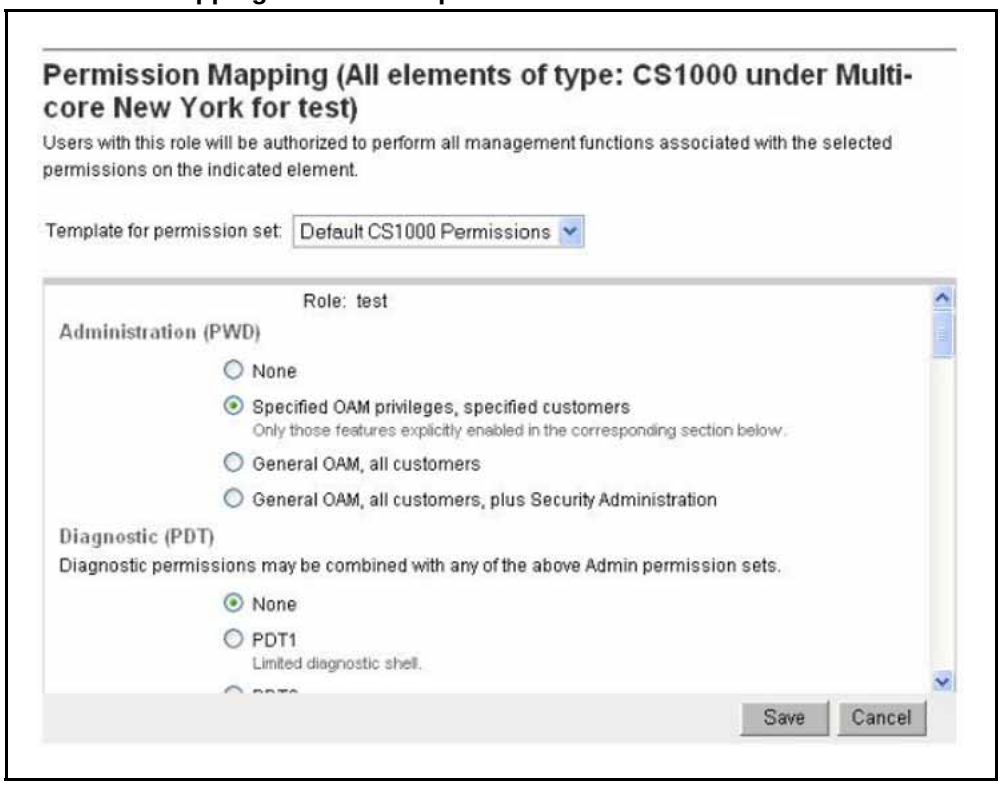
Depending on the element type that is selected, you may see different Permission Mapping pages, as shown in Permission

mapping —with element of type CS1000 and Permission Mapping—with element type of LinuxBase.

The Group Name selection is optional. You do not have to change the default selection of No Group Selected. If you do not select a Group Name, the available Element types are individual elements by name, elements by type, and network service.

If you select a group from the Group Name list, the Element and/or Network Service Name list shows only the types (not instances) of all available elements. The title of the Permission Mapping page changes to indicate the selected group, as shown in the following figure.

Figure 63
Permission mapping when a Group Name is selected

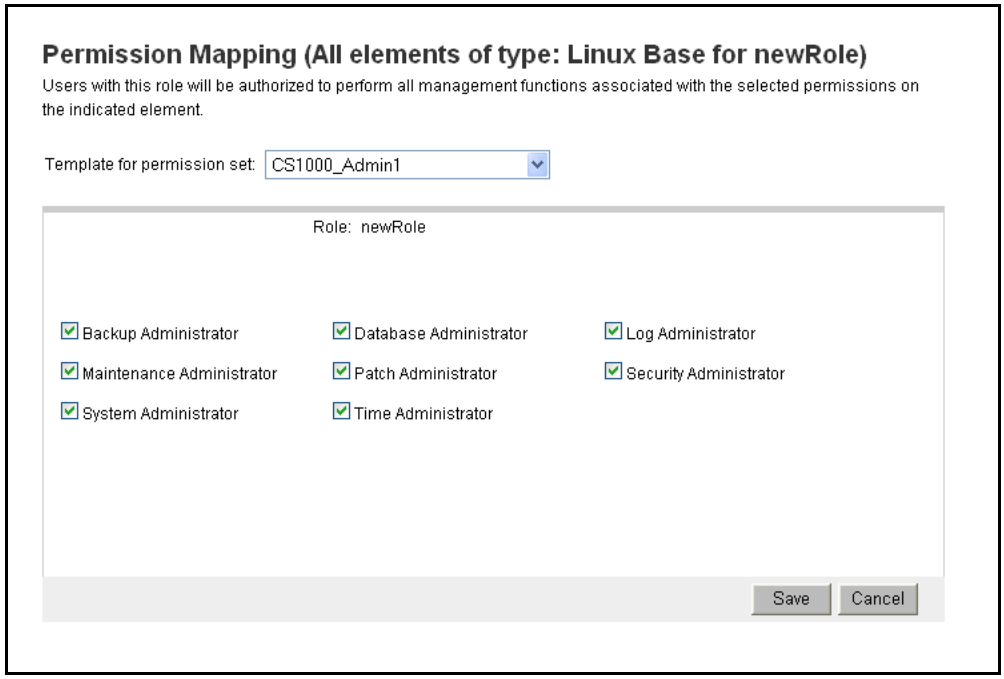


10 Permission mappings are divided into sections and boxes which varies for each Element type. Select the options required for this new role and click **Save**.

OR

11 The permission mapping page appears, as shown in the following figure.

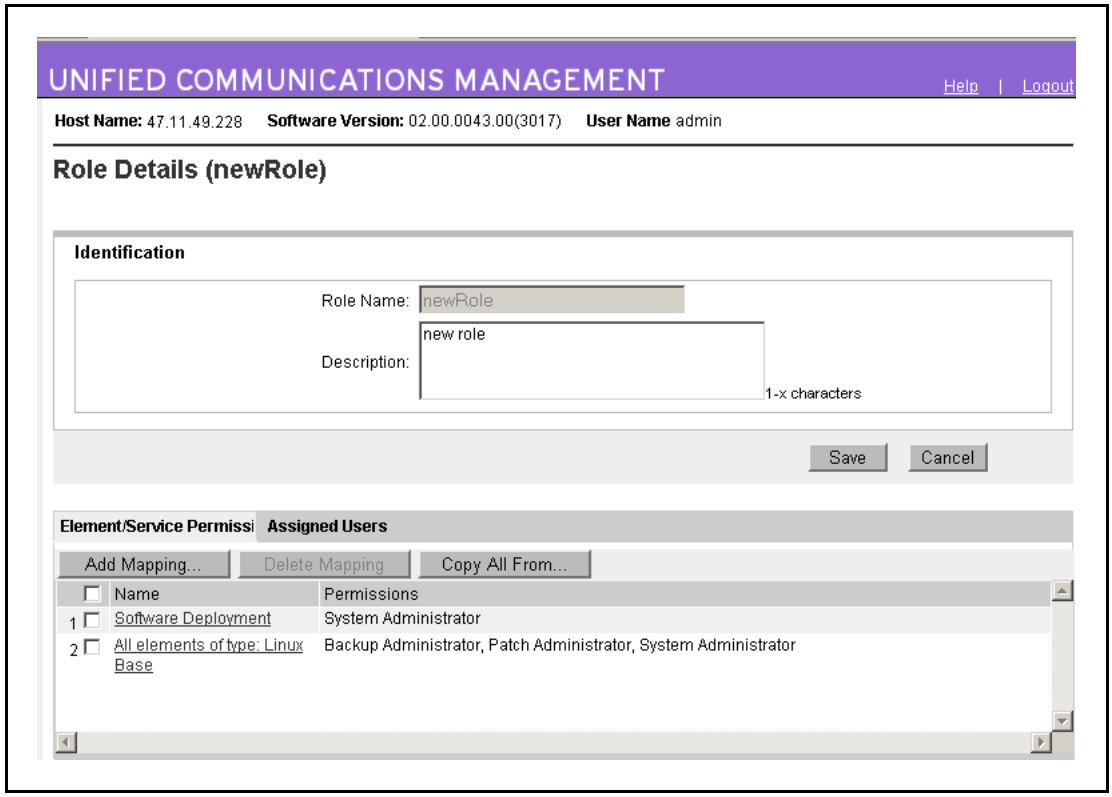
Figure 64
Permission Mapping—with element type of LinuxBase



12 Assign permissions for this role by selecting one or more check boxes. If there is a list beside the permission name, the administrator has the option to deny, modify, or view option for the permission associated with the role. Click **Save**.

13 The Role Details (newRole) page appears to confirm your settings, as shown in the following figure.

Figure 65
Role Details page with Assigned Users tab



--End--

Using templates for permission mapping

You can assign permissions by selecting a preconfigured permission template or you can create a custom permission template. A custom permission template can be created for a given element type by creating a custom role that maps to all elements of a given type, editing, and saving the permission mapping for all elements of a given type. The custom permission template then has the name of the custom role to where it belongs and appears in the Template for permission set option list, as shown in Figure 66 "Modifying the permission mapping " (page 138). The Permission mapping template also contains built-in roles to mapping permissions for an individual element or for all elements of a given type.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **Security, Roles**.

The Roles Web page appears, as shown in Figure 59 "Roles Web page" (page 132).

3 Click a role from the **Role Name** column.

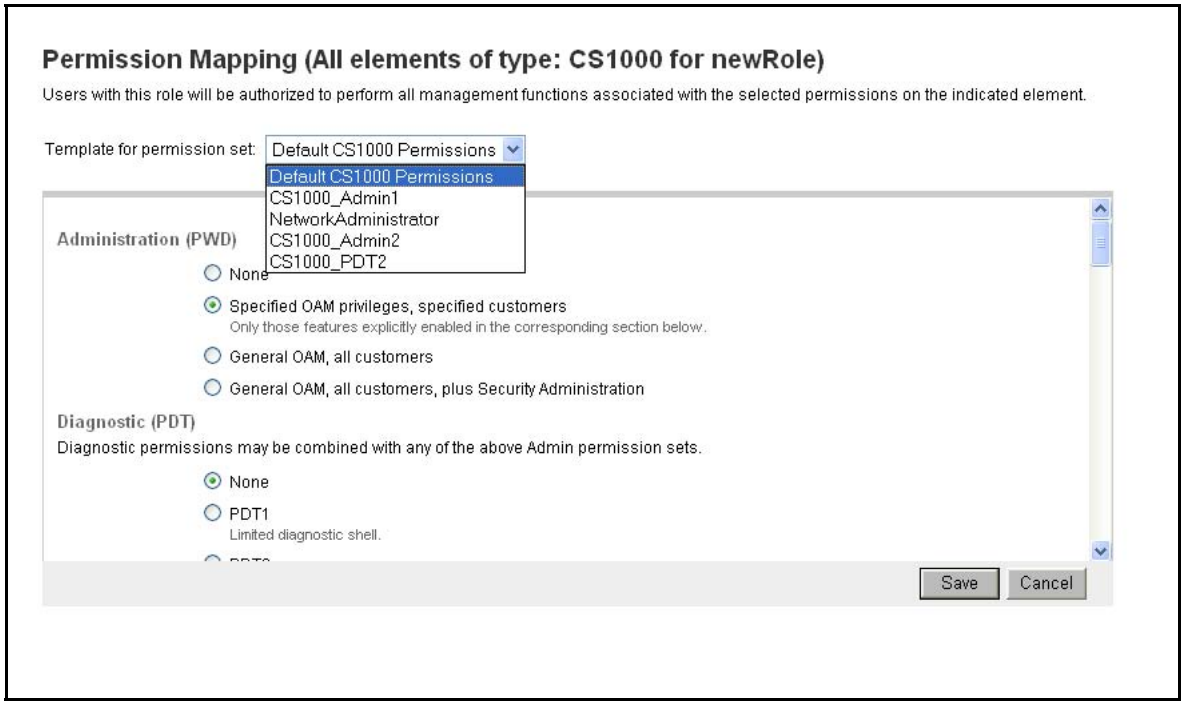
4 Click the **Element/Service Permissions** tab and click **Add Mapping**.

5 Select an Element Name, for example, CS1000, from the list and click **Next**.

The Permission Mapping (All elements of type: CS1000 for newrole) appears.

6 You can modify the permissions by selecting or clearing check boxes. You can also select another permission set by choosing another template from the list, as shown in the following figure.

Figure 66
Modifying the permission mapping



7 Click **Save**.

--End--

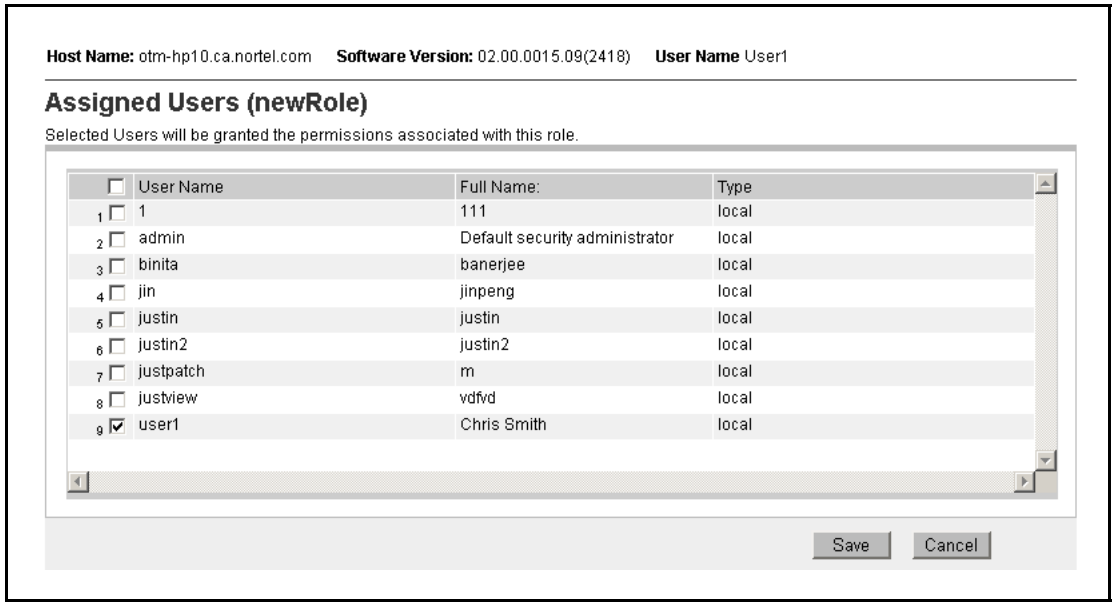
Assign or edit role mapping

The following procedures are used to assign or edit permission mapping. In the Role Details page, click the Assigned Users tab. There are two options for assigning permission mapping to a role. The administrator can select an element to add to a role by clicking Select Users or by copying the mapping from another role by selecting Copy all From.

Selecting users

Step	Action
1	In the **Assigned Users** tab.
2	Click **Select Users** to assign or edit a role to individual users. The Assigned Users (newRole) page appears, as shown in the following figure.

Figure 67
Assigned Users



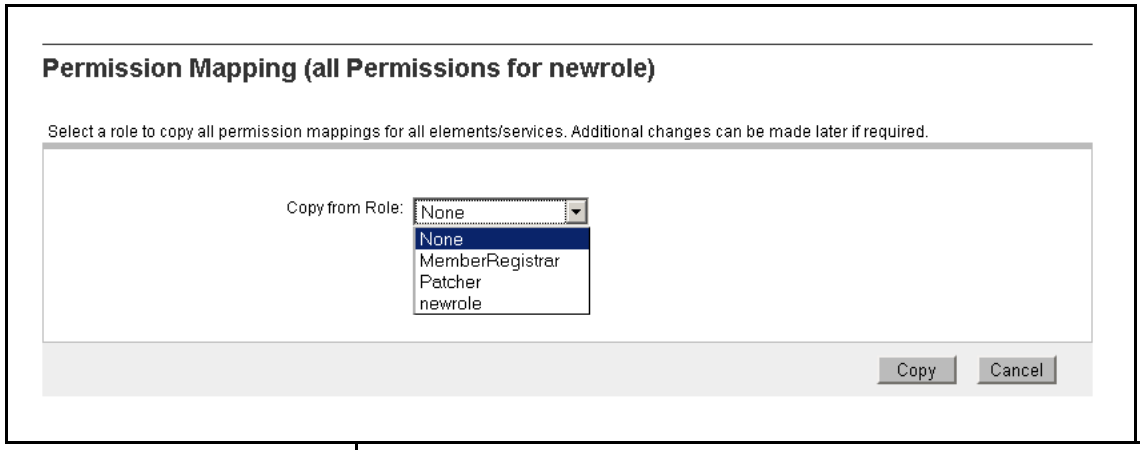
Step	Action
3	Select one or more check boxes beside the User ID to grant permissions associated with this role.
4	Click **Save**. The Role Details (newRole) page appears, as shown in Role Details page with Assigned Users tab. You can use this page to view the new permissions for that role.

--End--

Copying user assignment

Step	Action
1	An administrator can copy user assignments from another role to the new role. In the **Assigned Users** tab, click **Copy All From**.
2	The Permission Mapping (all Permissions for newrole) page appears, as shown in the following figure.

Figure 68
Permission Mapping (all Permissions for newrole)



ATTENTION
The copy from Role list does not contain the NetworkAdministrator role. The NetworkAdministrator role has underlying permissions that cannot be copied.

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

4 Click **Copy**.

The Role Details (newRole) page appears, as shown in Role Details page with Assigned Users tab.

5 Click **Save**.

The Roles page appears, as shown in Figure 59 "Roles Web page" (page 132). You can use this page to view the new permissions for that role.

--End--

Editing a role description

Edit the role description, Element/Service Mapping, and Assigned Users. The role name cannot be changed from the Role Details page.

Step	Action
1	Log on to UCM.
2	On the navigation tree, click **Security**, **Roles**. The Roles Web page appears, as shown in Figure 59 "Roles Web page" (page 132).
3	In the **Role Name** column, click a Role Name item to edit the description.

The Role Details (newRole) Web page appears, as shown in Role Details (newRole).

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

5 Click **Save** to save your changes or **Cancel** to return to the Roles page without saving your changes.

The Roles Web page reappears, as shown in Figure 59 "Roles Web page" (page 132).

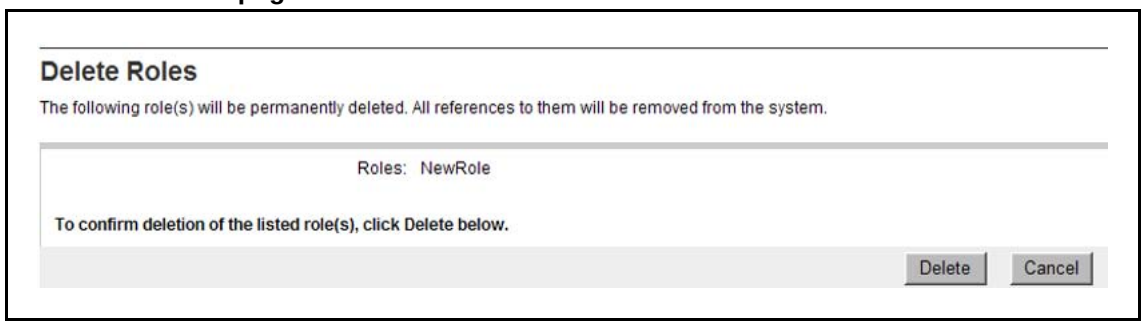
--End--

Deleting custom roles

Only custom roles can be edited or deleted. Log on as network administrator to delete a custom role. User role assignments for administrators assigned to the deleted roles are also deleted.

Step	Action
1	Log on to UCM as a network administrator.
2	On the navigation tree, click **Security**, **Roles**.
3	In the **Roles** Web page, select one or more check boxes beside the custom role to delete. The Delete Roles Web page appears with the selected roles for deletion, as shown in the following figure.

Figure 69
Delete Roles Web page



4 Click **Delete** to proceed with the deletion or **Cancel** to cancel the deletion and return to the Roles page.

--End--

Policies

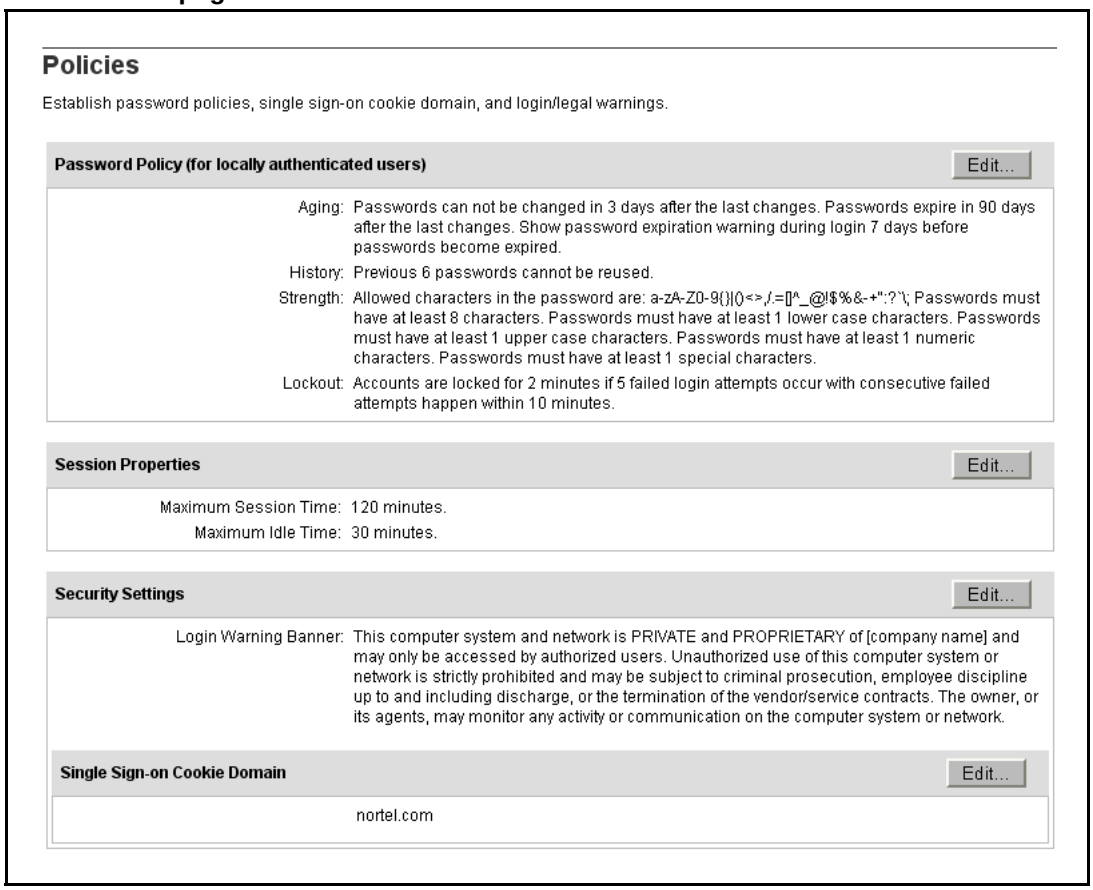
In the Security branch of the navigation tree, click Policies. The Policies Web page appears. A network administrator can configure the Password policy (for locally authenticated users), Security Settings, and the Single Sign-on (SSO) Cookie Domain.

Reviewing security policies

Review the currently configured security policies within the UCM.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **Security**, **Policies**. The Policies Web page appears, as shown in the following figure.

Figure 70
Policies Web page



3 Review the policy settings currently in UCM.

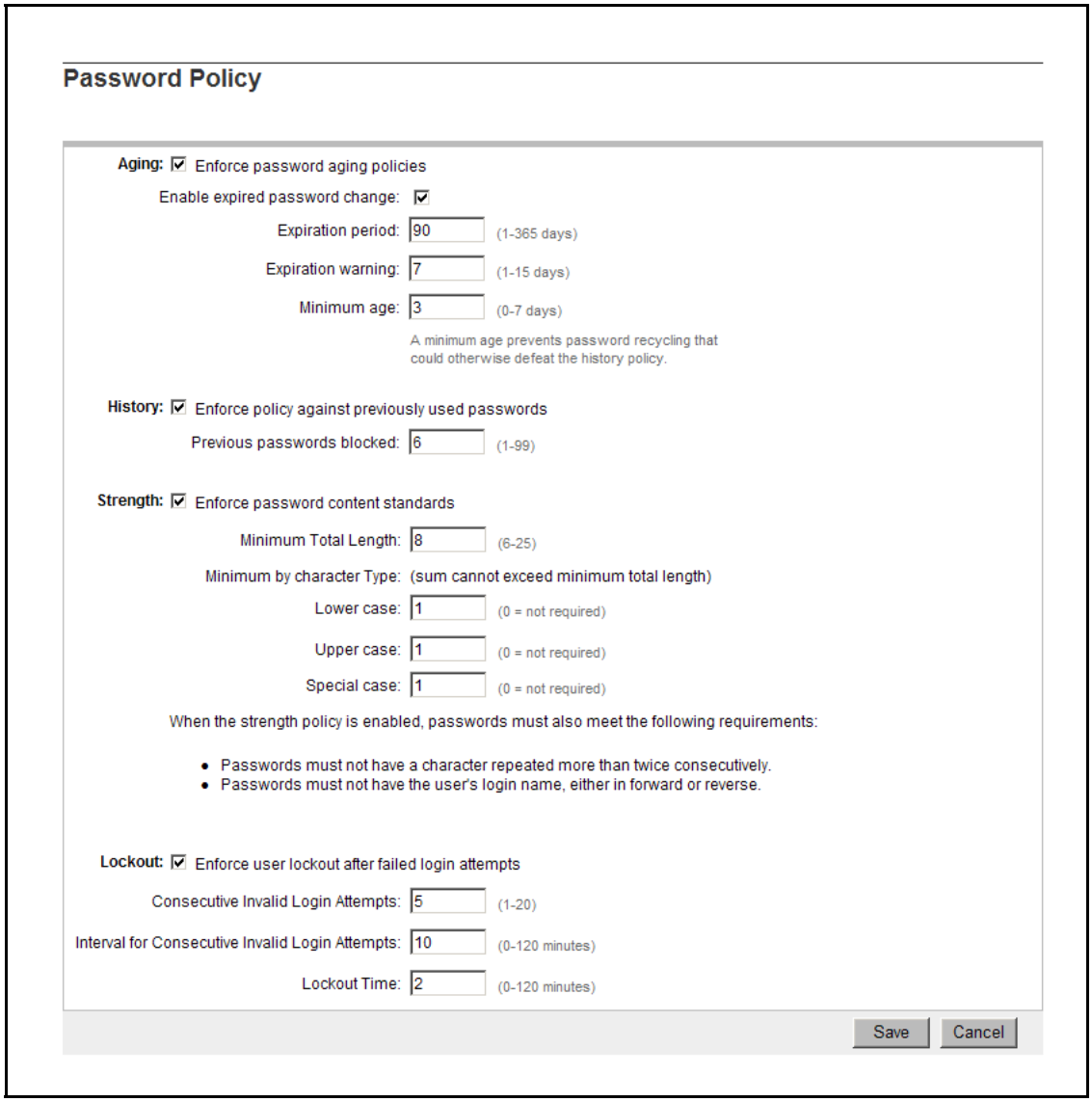
--End--

Editing password policies

Configure the local account password policies including, aging, history, strength, and lockout password policies in UCM according to business requirements.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Policies**. The Policies Web page appears, as shown in Figure 70 "Policies Web page" (page 142).
3	In the Password Policy (for locally authenticated users) section, click **Edit**. The Password Policy Web page appears, as shown in the following figure.

Figure 71
Password Policy Web page



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

- Select the **Aging** check box.
- In the **Expiration period** field, type a number from 1 to 365 for the maximum allowable days to maintain 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 from 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 greater than the minimum password age number.

ATTENTION
All passwords expire. If an administrator password expires, the administrator can reset the password through the UCM user interface.

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

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

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

- Select the **Strength** check box.
- In the **Minimum Total Length** field, type a number from 6 to 25 for the minimum number of total characters for the password. The default value is 8.
  In the **Minimum by character Type** fields, perform the following steps:
  - In the **Lower case** field, type the minimum number of lowercase characters for the password. The default value is 1.
  - In the **Upper case** field, type the minimum number of uppercase characters for the password. The default value is 1.
  - In the **Numeric case** field, type the minimum number of numeric characters for the password. The default value is 1.
  - In the **Special case** field, type the minimum number of special characters for the password. The default value is 1.

ATTENTION
The sum of the character types cannot exceed the minimum total length.

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

- Select the **Lockout** check box.
- In the **Consecutive Invalid Login Attempts** field, type a number for failed attempts from 1 to 20. The default value is 5.

- In the **Interval for Consecutive Invalid Login Attempts** field, type the interval in number of minutes from 0 to 120 for consecutive invalid logon attempts. The default is 10 minutes.
- In the **Lockout Time** field, type the number of minutes from 0 to 120 until the account is unlocked. The default is 2 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 is reached.
- The password is expired.

For each scenario, the system responds with a message that invalid logon credentials were used. You must contact the network administrator for additional information.

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

8 Click **Save**.

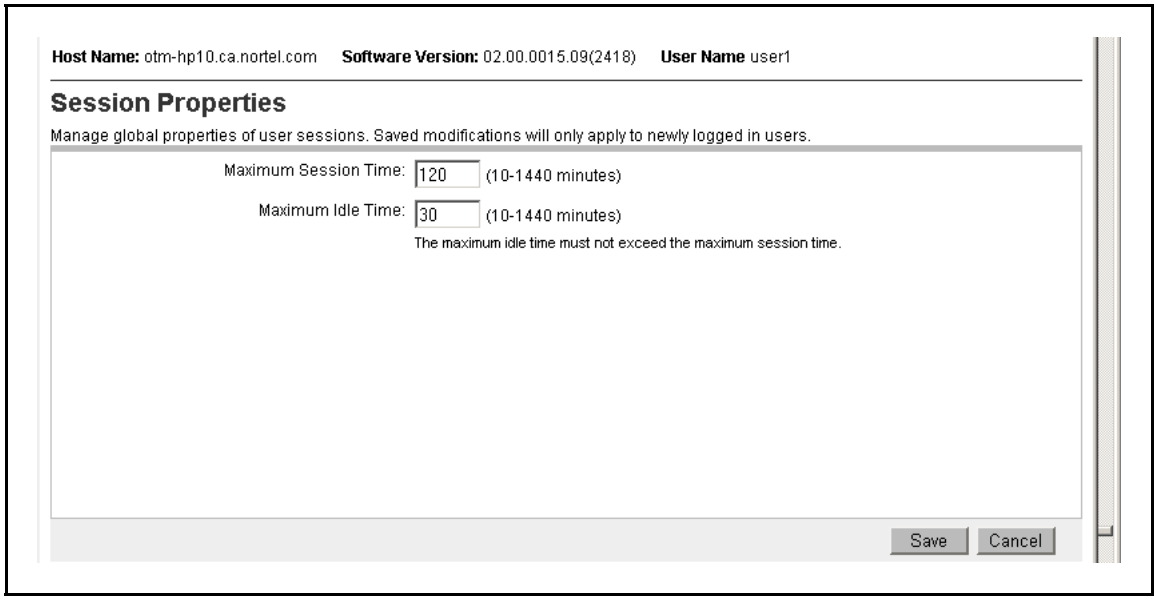
--End--

Editing Session Properties

Manage the global properties of user sessions including maximum session time and maximum idle time.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Policies**. The Policies Web page appears, as shown in Figure 70 "Policies Web page" (page 142).
3	In the Session Properties section, click **Edit**. The Session Properties page appears, as shown in the following figure.

Figure 72
Session Properties



4 Perform the following actions:

- In the **Maximum Session Time** field, type a number for maximum session time in minutes from 0 to 1440.
- In the **Maximum Idle Time** field, type a number for the maximum idle time in minutes from 0 to 1440.

5 Click **Save**.

--End--

Security Settings

UCM provides a customizable logon banner that appears when a user logs on to the system. The customizable banner is intended for use by customers with security policies that require network equipment to display a specific message to users when they log on. The following figure show the default logon warning banner message.

Table 12
Default Login warning message

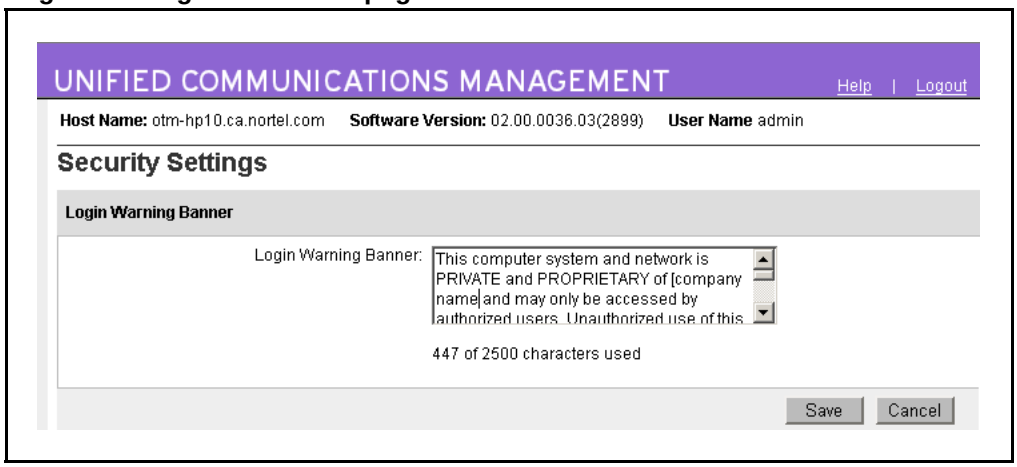
WARNING! This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge,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

Editing the login warning banner

Customize the message for the logon warning banner in UCM.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Policies**. The Policies Web page appears, as shown in Figure 70 "Policies Web page" (page 142).
3	In the **Security Settings** section, click **Edit**. The Logon Warning Banner Web page appears, as shown in the following figure.

Figure 73
Login Warning Banner Web page



Step	Action
4	In the **Login Warning Banner** text area, edit the text as required. ***Note:*** The maximum number of characters allowed is 2500.
5	Click **Save**.

--End--

Editing the Single Sign-on Cookie Domain

Change the Single Sign-on (SSO) cookie domain when the primary and backup security servers are configured in different domains, Single Sign-on (SSO) requires authentication to switch from the primary to backup security server. For authentication, the primary and backup security server domain names must match.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Policies**. The Policies Web page appears, as shown in Figure 70 "Policies Web page" (page 142).
3	In the **Single Sign-On Cookie Domain** section, click **Edit**. The Edit Domain Name page appears, as shown in the following figure.

Figure 74
Edit Single Sign-On Cookie Domain Web page

4	From the **Single Sign-On Cookie Domain** list, select a URL to change the Single Sign-on Cookie Domain.
5	Click **Save** to save the change or **Cancel** to discard the change.

--End--

ATTENTION

- When the SSO cookie domain changes, you must clear the existing UCM related cookies from the cache in the Internet browser for all users.
- When selecting an SSO cookie domain, ensure that all servers in the security domain share the same cookie domain. For example, if you are in the domain ca.nortel.com and you want to access servers using single sign-on in the domain europe.nortel.com, you need to change the SSO to nortel.com.
- Top level domains such as com.ca or com.au cannot be assigned as the SSO cookie domain as these can be rejected by some Internet browsers.

Certificates

In the Security branch of the navigation tree, click Certificates. The Certificate Management Web page appears. From the Security Certificates Web page, a network administrator can access the Certificate Endpoints tab and the Private Certificate Authority tab, as shown in Figure 75

"Certificate Management" (page 151).You can search and filter a certificate endpoint by typing an endpoint friendly name or endpoint address.
You can search and filter all certificates generated by the UCM private certificate authority from the Certificate Management page by typing the certificate serial number or subject DN. The search field can be used to search Certificate Endpoints as well as the certificates generated by the UCM private CA. For a successful endpoint search, the search criteria must contain at least a part of an Endpoint Address or Element Name. For a successful certificate search, the search criteria must contain at least a part of the certificate Serial Number or Subject DN.

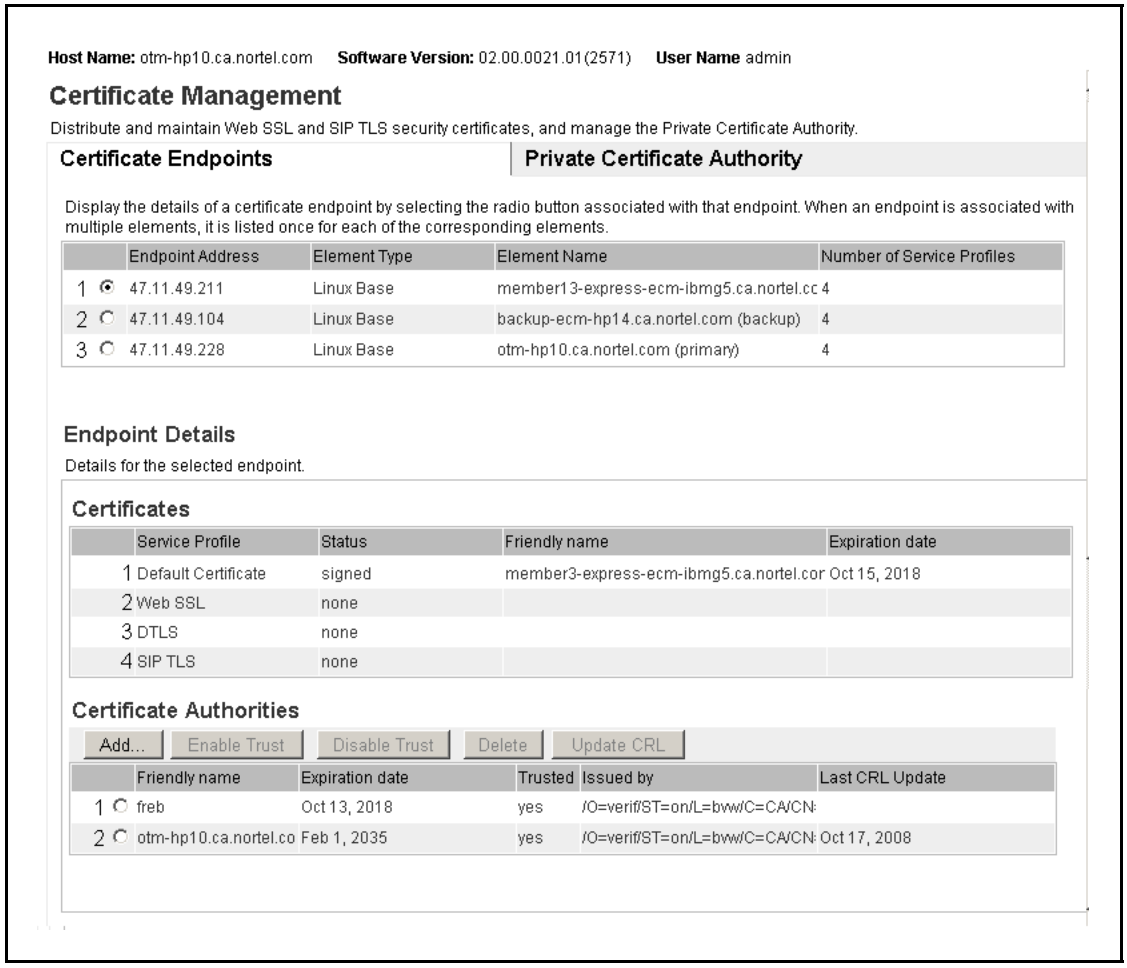
Perform the following procedures to view the Certificate Endpoints and the Private Certificate Authority. For more information about certificates, see *Nortel Security Management Fundamentals* (NN43001-604).

Viewing the details of a certificate endpoint

View the details of a certificate endpoint.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	In the navigation tree, click **Security**, **Certificates**.
	The Certificate Management Web page appears, as shown in the following figure.

Figure 75
Certificate Management



3 In the Certificate Endpoints section, click the option next to the endpoint for which you want to view the details.

The certificate information related to the selected endpoint appears in the Endpoint Details section. To access the service profile , click the Service Profile column header.

--End--

Updating the CRL

Update a CRL for a certificate endpoint.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Certificates**.

The Certificate Management Web page appears, as shown in Figure 75 "Certificate Management" (page 151).

3 In the Certificate Authorities section, click the option button next to the certificate authority for which you want to update the CRL.

4 Click **Update CRL**.

5 A popup window appears.

6 Copy the contents of the CRL and paste in the text area.

7 Click **Submit**

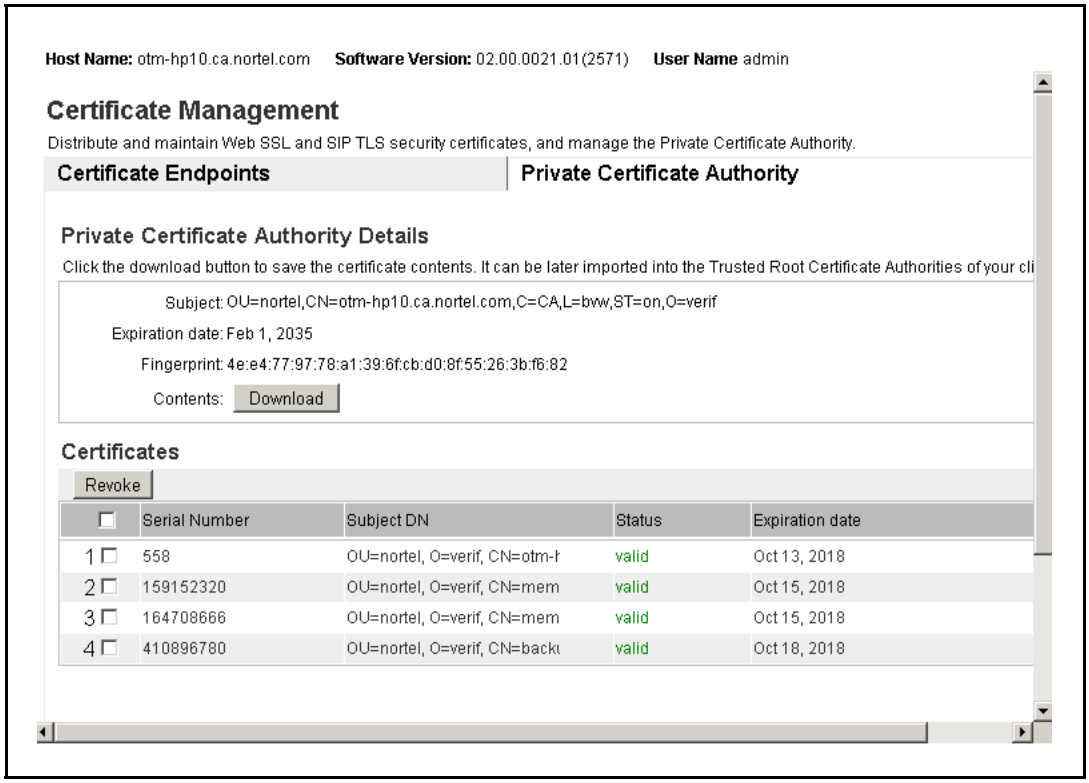
--End--

Downloading Private Certificate Authority Details

Use the Private Certificate Authority tab to display a list of all the issued and revoked certificates.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Certificates**. The Certificate Management Web page appears, as shown in Figure 75 "Certificate Management" (page 151).
3	Click the **Private Certificate Authority** tab. The Private Certificate Authority window appears, as shown in the following figure.

Figure 76
Private Certificate Authority



4 In the Private Certificate Authority Details section, click **Download** to download the certificate contents as a security certificate file.

The File Download - Security Warning window appears.

5 Click **Save**.

The Certificate Details window appears showing the details of the certificate.

6 Click **Ok**.

--End--

Revoking a certificate

Revoke a certificate.

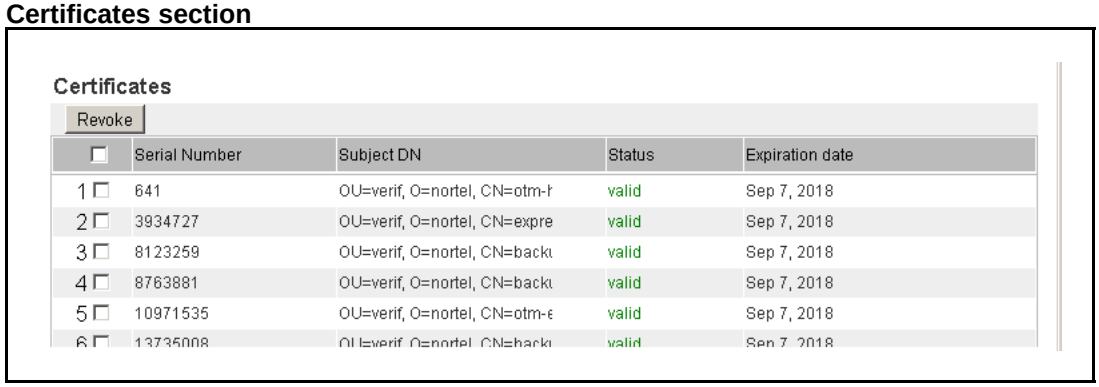
Step	Action
1	Log on to UCM Common Services as administrator.
2	On the navigation tree, click **Security**, **Certificates**.

The Certificate Management Web page appears, as shown in Figure 75 "Certificate Management" (page 151).

3 Click the **Private Certificate Authority** tab, as shown in Figure 76 "Private Certificate Authority" (page 153).

4 In the Certificates section, select one or more of the check boxes beside the Serial Number and click **Revoke** to revoke the selected certificates, as shown in the following figure.

Figure 77
Certificates section



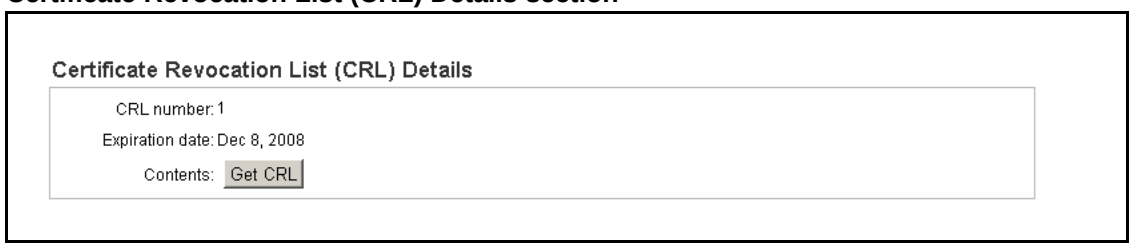
--End--

Downloading the Certificate Revocation List (CRL) Details

Download details of the Certificate Revocation List.

Step	Action
1	Log on to UCM Common Services as a network administrator.
2	On the navigation tree, click **Security**, **Certificates**. The Certificate Management Web page appears, as shown in Figure 75 "Certificate Management" (page 151).
3	Click the Private Certificate Authority tab.
4	In the Certificate Revocation List (CRL) Details section, click **Get CRL**, as shown in the following figure.

Figure 78
Certificate Revocation List (CRL) Details section



The File Download window appears.

5 Click **Save**.

--End--

Adding a CallPilot certificate

The CallPilot certificate must be added to the UCM manually. The Web browser cannot prompt a user to accept a certificate when communicating internally between UCM and CallPilot because CallPilot is not integrated in the UCM security framework. Use the following procedure to manually add the CallPilot certificate.

Step	Action
1	In the Internet Explorer Web browser, type **https://<CallPilot IP>/cpmgr**. Where <CallPilot IP> is the IP or FQDN of the CallPilot Manager requiring the certificate.
2	For Internet Explorer 6.0: In the Security Alert dialog box, click **View Certificate** and go to Step 6. For Internet Explorer 7.0 or 8.0: Click **Continue to this website (not recommended)**. The CallPilot Manager page appears.
3	When the certificate is signed by a Trusted Certificate Authority, right-click the lock icon that appears to the right of the Web address bar.
	OR
4	When the certificate is not signed by a Trusted Certificate Authority, right-click **Certificate Error** on the pink bar, as shown in the figure below.

Figure 79
Certificate Error

5 Click **View Certificates**.

The Certificate window appears.

6 Click the **Details** tab.

7 In the Certificate export Wizard window, click **Copy to File** and click **Next**.

8 Select the **Base-64 encoded X.509 (.CER)** option and click **Next**.

Select a directory and type a file name for the certificate and click **Next**.

9 Click **Finish** to exit the Certificate Export Wizard.

10 Log on to UCM. In the UCM navigation tree, click **Security**, **Certificates**.

The Certificate Management Web page appears.

11 On the Certificate Endpoints tab, click the option button next to the endpoint address for which you want to view the details. In this case, the UCM server.

12 In the Certificate Authorities section, click **Add**.

13 Open the .CER file from Step 8 in a text editor and copy the contents into the **Add a CA to the Service dialog** box and click **Submit**.

14 The CallPilot certificate is displayed in the Certificate Authorities table and all communication to the CallPilot is secured over SSL.

15 Log off and log on to UCM for the change to take affect.

--End--

Active Sessions

Access the Active Sessions Web page from the Security branch of the UCM navigation tree to review user session information and to terminate user sessions. With the appropriate permissions, a network administrator can view the session information for any user who is currently logged on.

Viewing active sessions

View the current sessions in UCM. Network administrators can see all users who are currently logged on to UCM and view the session time for the user.

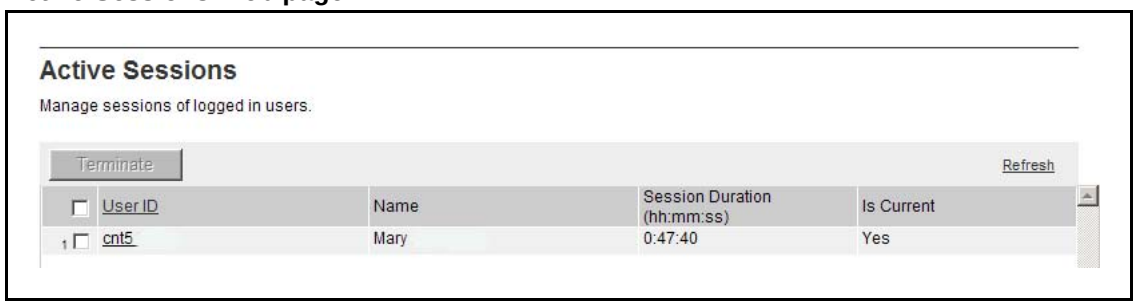
Step	Action
1	Log on to UCM as a network administrator.

2 On the navigation tree, click **Security**, **Active Sessions**.

The Active Sessions Web page appears, as shown in the following figure.

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

Figure 80
Active Sessions Web page



--End--

Terminating Single Sign-On sessions

Terminate selected Single Sign-On (SSO) sessions in UCM.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **Security**, **Active Sessions**. The Active Sessions Web page appears, as shown in Figure 80 "Active Sessions Web page" (page 157).
3	Select the check box beside the required sessions to terminate.
4	Click **Terminate**. The selected sessions are deleted from the current sessions table. Administrators with terminated sessions are required to log on again.

--End--

UCM Tools configuration

This chapter contains information on the Tools branch in the Unified Communications Management (UCM) navigation pane.

Navigation

Logs

Access the Logs Web page from the Tools branch of the UCM navigation tree to view log files. You can view logs by OAM Events and Security Events type, use the date or search function, configure or edit the configuration of logs for third-party OSS, and export the logs as comma-separated value (CSV) files. From Base Manager, you can also configure forwarding of logs that are generated on the backup and member servers for consolidation on the primary security server.

ATTENTION
The Security Event log type and Log Forwarding button are not available when you are logged on as a non-network administrator.

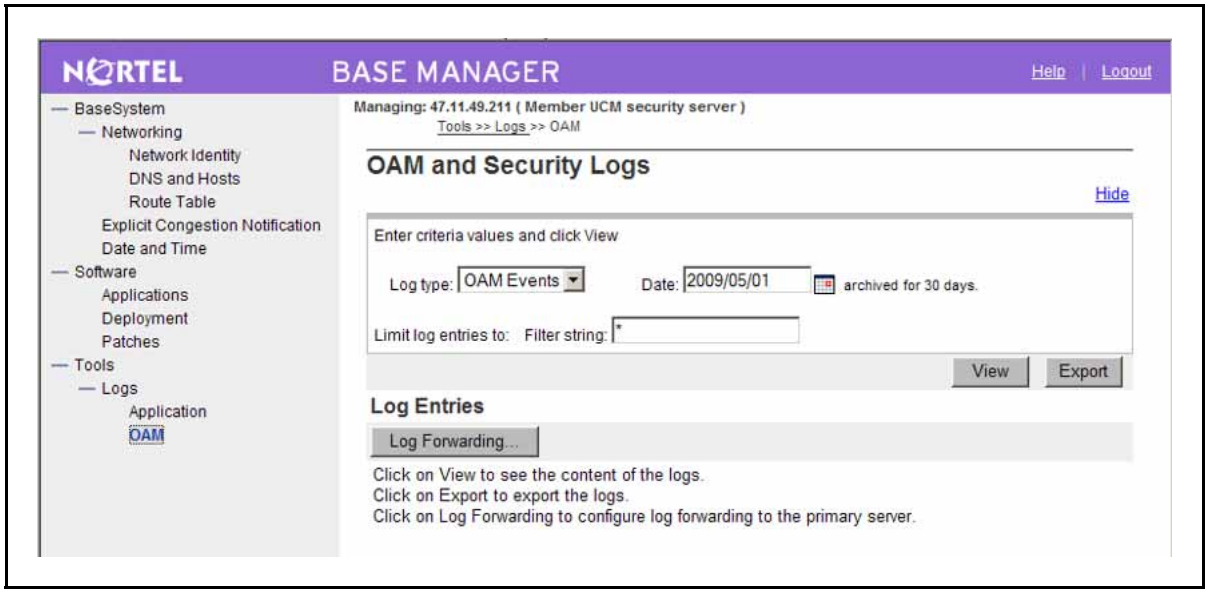
Enabling OAM and Security logs for consolidation

Configure consolidation of OAM and Security logs to the primary security server from the backup and member security server.

ATTENTION
By default, log consolidation is not configured.

Step	Action
1	Log on to the UCM member security server as a network administrator to access Base Manager.
2	On the navigation tree, click **Tools, Logs, OAM**, as shown in the following figure.

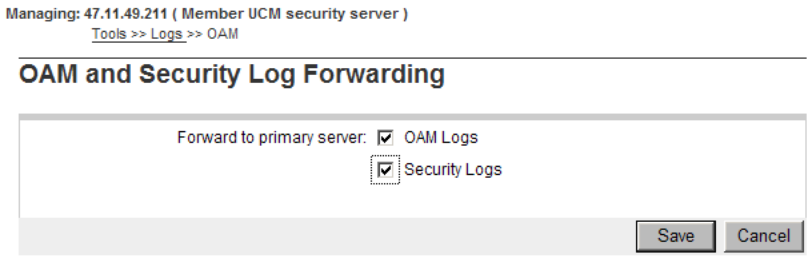
Figure 81
Log Forwarding Base Manager



3 Click **Log Forwarding**.

The Log consolidation Web page appears, as shown in the following figure.

Figure 82
Logs consolidation Web page



4 In the **Forward to primary server** field, select **OAM logs** and **Security Logs** to enable consolidation of logs.

5 Click **Save**.

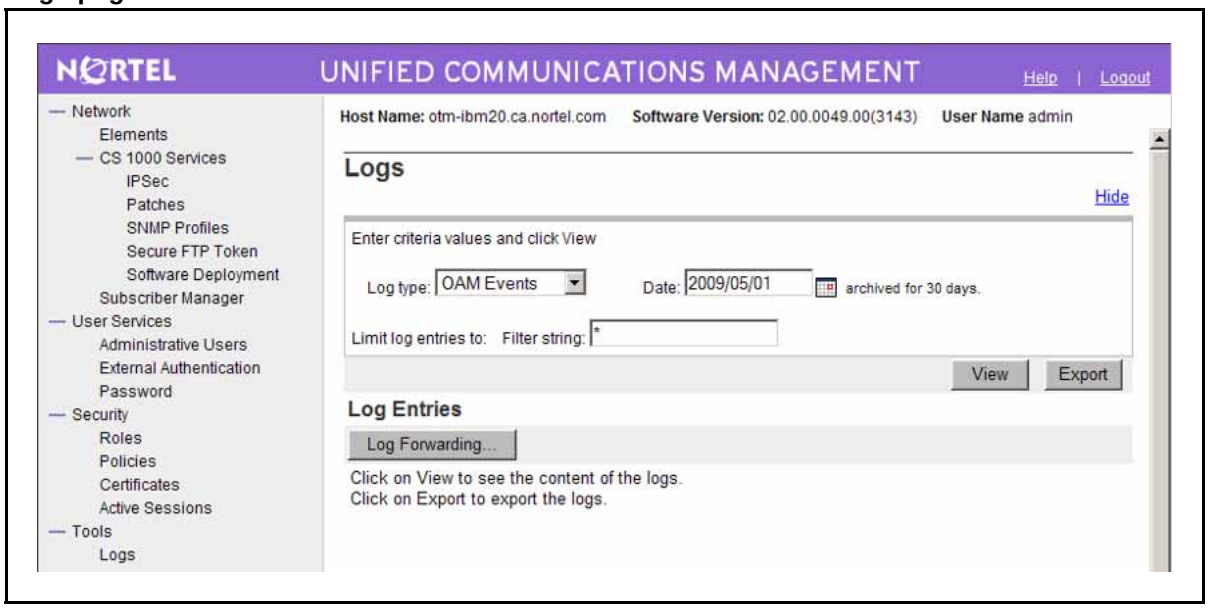
--End--

Viewing log types with the network administrator role

View log types when you log on with the network administrator role.

Step	Action
1	Log on to UCM as a network administrator.
2	In the navigation tree, click **Tools**, **Logs**. The Logs Web page appears, as shown in the following figure.

Figure 83
Logs page with network administrator role



3	In the **Log type** field, select **OAM Events** or **Security Events** from the list.
4	Click **View**.

--End--

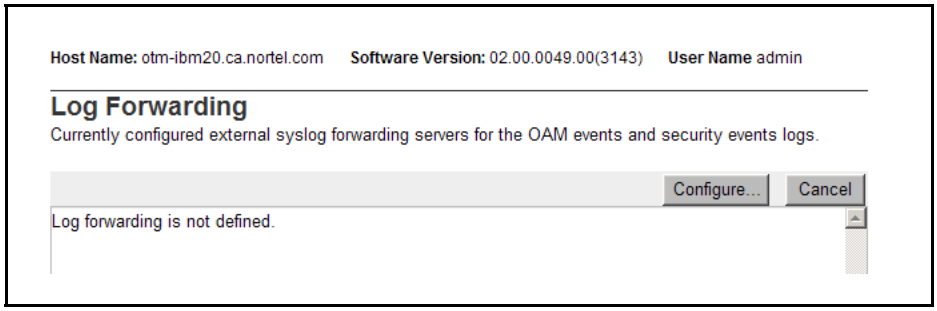
Configuring or editing the configuration of logs for forwarding to third-party OSS

Configure or edit the configuration of logs for forwarding to third-party Operational Support System (OSS) Syslog servers when you log on with the network administrator role. Network administrators can forward OAM Events and Security Event logs.

ATTENTION
Application logs from any type of server cannot be forwarded to third party OSS. When configuring member and primary servers between a firewall or SMC, the firewall must be enabled with the syslog port UDP 514 to allow the messages from the members to reach the primary.

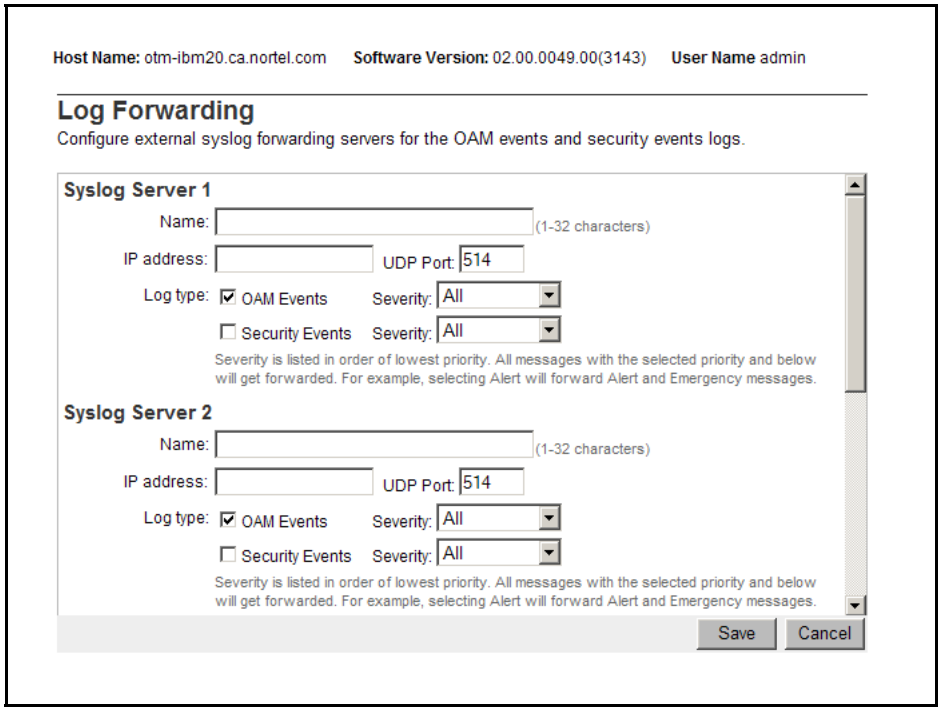
Step	Action
1	Log on to UCM as a network administrator.
2	On the navigation tree, click **Tools**, **Logs**. The Logs Web page appears, as shown in Figure 83 "Logs page with network administrator role" (page 161).
3	Click **Log Forwarding**. The Log Forwarding page appears, as shown in the following figure.

Figure 84
Log Forwarding



4	Click **Configure** to configure log forwarding. The Log Forwarding configuration page appears, as shown in the following figure.

Figure 85
Configuring log forwarding



5 Configure external syslog forwarding servers by completing the following fields:

Name Type hostname of the third party system. It must be between 1 to 32 characters.

IP address Type the IP address of the syslog server.

UDP port Type the UDP port number of the syslog server. Default is 514.

Log type Select **OAM Events** and choose the Severity from the list (options are: All, Debug, Information, Notice, Warning, Error, Critical, Alert, Emergency)

OR

Select **Security Events** as the Log type.

ATTENTION
Severity is listed in order of lowest priority. All messages with the selected priority and the priorities below it are forwarded, for example, selecting Alert forwards Alert and Emergency messages.

6 Click **Save**.

--End--

Viewing audit logs by date

View logs by selecting a date.

Step	Action
1	Log on to UCM.
2	On the navigation tree, click **Tools**, **Logs**. The Logs Web page appears, as shown in Figure 83 "Logs page with network administrator role" (page 161).
3	In the **Date** field, type a date within the last 30 days using the format YYYY/DD/MM, or click the calendar icon to select a date.
4	Click **View**. The results of the search appear on the same page.

--End--

ATTENTION
The selected date cannot be older than 30 days from the current date; otherwise, an error message appears.

Viewing Audit logs using the search functionality

View logs using the search functionality.

Step	Action
1	Log on to UCM.
2	On the navigation tree, click **Tools**, **Logs**. The Logs Web page appears, as shown in Figure 83 "Logs page with network administrator role" (page 161).
3	In the **Limit log entries to** section, type a search string in the **Filter string** field. For example, info.
4	Click **View**. The results of the search appear on the same page.

--End--

Exporting the log file as a CSV file

Export the log file as a CSV file.

ATTENTION
Non-network administrators can export only OAM event logs.

Step	Action
1	Log on to UCM.
2	On the navigation tree, click **Tools**, **Logs**. The Logs Web page appears, as shown in Figure 83 "Logs page with network administrator role" (page 161).
3	Click **Export**. The File Download dialog box appears.
4	Click **Save** to export the log file as a CSV file.

--End--

Index

Nortel Communication Server 1000

Unified Communications Management Common Services Fundamentals

Release: 7.0
Publication: NN43001-116
Document revision: 04.01
Document release date: 4 June 2010

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

www.nortel.com