NORTEL

Nortel Communication Server 1000

Security Management Fundamentals

Release: 6.0
Document Revision: 03.08

www.nortel.com

NN43001-604

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-604
Document release date: 14 April 2010

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New in this release 11
Other changes 11
Revision history 11

How to get help 15
Getting help from the Nortel Web site 15
Getting help over the telephone from a Nortel Solutions Center 15
Getting help from a specialist by using an Express Routing Code 16
Getting help through a Nortel distributor or reseller 16

Introduction 17
Purpose 17
Navigation 18
Other security information 18
About this document 19
Subject 19
Intended audience 20
Terminology conventions 20

Fundamentals of system security management 21
System security overview 23
General signaling security overview 23
Key management concepts 23
Public-key certificate concepts 25
Platform security overview 28
Unified Communications Management security services 28
Unified Communications Management security server roles 29
Security Domain Manager concepts 30
Linux security hardening 31
Internal communications security overview 36
ISSS/IPsec 36
Secure File Transfer Protocol concepts 38
Port access restrictions concepts 40
Linux Master Firewall Control 41
Media and signaling security overview 42

Media Security concepts 42
TLS security for SIP trunks concepts 44
UNIStim signaling encryption with DTLS 44
NRS SIP Proxy 44
User and password management concepts 45
OAM overview 45
Access control management 47
System upgrade password conversion 48
Global password settings 48
Role management in Unified Communications Management 49
Security administration concepts 49
SSH and secure remote access 49
Customizable logon banner 49

Recommended security practices 51
Recommendations for OAM security 51
Recommended password management practices 52
Upgrading user names from an earlier release 52
Recommendations to protect confidentiality 53
ISSS/IPsec recommendations 53
Preshared keys, SSH keys, and Secure FTP Token recommendations 53
TLS security for SIP trunks recommendations 54
Media Security recommendations 54
Recommendations for security administration 54
Shell Access Control 54
Certificates 55
Security code for Mobile Extensions 55
Single sign-on cookie domain 55
Certificate management 56
Upgrade from an earlier release 56
Recommendations to protect UNIStim IP Phones 57
UNIStim with DTLS recommendations 57
Prevent GARP spoof attacks 57
Enable layer 2 authentication for IP Phones 58
Sign files 58
Security interactions 58
Co-resident CP PM Call and Signaling Server 59
ISSS and Element Manager on VxWorks signaling server 59
ISSS and Element Manager on UCM 60
ISSS and Geographic Redundancy 60
ISSS and AML 61
ISSS and Port Access Restrictions and Linux firewall 61
ISSS and other protocols 62
Media Security and call forwarding 62

Media Security and SIP phones 62
Media Security Always and CallPilot mailboxes on systems without MGC daughterboards or MC32S 63
SIP TLS security policy interaction with Failsafe NRS 63
SIP TLS interaction with SMC 2450 64
Recommendations for upgrading to Communication Server 1000 Release 6.0 from a previous release 64
Prerequisites 64
Migrate existing CS 1000 Release 5.x user accounts to CS 1000 Release 6.0 66
Prerequisites 66

ISSS 69
ISSS overview 69
Unified Communications Management IPsec ISSS management interface page 71
IPsec configuration 74
Prerequisites 74
Configure ISSS for a new installation 74
Configure default IPsec settings 76
Add a new manual IPsec target 78
Edit an existing manual IPsec target 79
Enable or disable IPsec for a target 80
Delete a manual target 81
Customize IPsec for a Call Server target 82
Activate IPsec configuration settings 84
Synchronize IPsec configuration settings 85
Configure ISSS when a new element joins the security domain 86
Other ISSS configuration and maintenance procedures 87
Maintenance on Linux servers 87
Manual ISSS configuration on each device 90

Certificate Management 95
Prepare the system for certificate management 95
CA management 96
Private CA Configuration 96
Add a CA to an endpoint 99
Change the trust status of an endpoint 101
Delete a CA 102
Certificate creation and management 103
Certificate information 105
Add a UCM server certificate to the Web browser 106
Create a certificate for Web SSL signed by the private CA 107
Create a certificate for Web SSL signed by a trusted third-party CA 112
Create a self-signed certificate for Web SSL 117
Create a certificate for SIP TLS signed by the private CA 123

Create a certificate for SIP TLS signed by a public CA 128
Create a request for a third-party CA certificate for SIP TLS when upgrading the system 133
Create a self-signed certificate for SIP TLS 140
Process a pending certificate response 144
Delete a pending certificate request 146
Create a certificate renew request for the current certificate 148
Export the current self-signed certificate 151
Export the current certificate and its private key 153
Import a certificate and its private key from a file 156
Assign an existing certificate 159
Replace the current certificate 161
Remove the current certificate 163
Revoke a certificate 165
Download the Certificate Revocation List (CRL) Details 166

SIP security 169
About TLS security for SIP trunks 169
SIP Lines 171
SIP TLS configuration overview 171
View SIP TLS configuration 174
Job aid: config.ini 174
TLS security for SIP trunks configuration using Element Manager 175
Configuring SIP TLS security policy 176
SIP TLS Certificate management 181
SIP TLS maintenance using CLI 181

Media Security 183
About Media Security 183
UNIStim with DTLS encryption 185
DTLS and IP Phone registration 186
Security levels 187
DTLS configuration options 188
UNIStim DTLS overlay commands 189
Configure UNIStim DTLS using Element Manager 190
Update UNIStim DTLS using Element Manager 193
View UNISTIM DTLS details using Element Manager 194
Key sharing 196
Protecting the media stream using SRTP PSK 196
Protecting the media stream using SRTP USK 196
Media Security configuration using Element Manager 196
System-wide Media Security configuration 196
VTRK Class of Service configuration 199
Media Security configuration using overlays 201
System-wide Media Security configuration 201

- Class of Service configuration 202
- VTRK Class of Service configuration 204

Media Security configuration information 205
- Media Security configuration information available using overlays 205
- Media Security information available using an IP Phone 207
- SIP Route information available using overlays 208

User and password management 209

Roles and permissions 210
- Inheritance of UCM role-based permissions for Element type of CS 1000 211
- Permission templates 211

Account types and roles 212
- Account synchronization 212
- Customer passwords 212

User and password management using overlays 214
- User management 214
- Password management 224
- Global password settings configuration 226
- Password reset 228
- Multi-user login configuration using overlays 231
- History File configuration using overlays 233
- Password management for stand-alone Signaling Server 233

User and password management using Element Manager 234
- Add a user 234
- Edit an existing user 239
- Synchronize a changed password 241
- Edit global password settings 242

Security administration 247

Control access to the system 247
- System administration port security 248
- Switchroom security 248
- Network facilities security 249

Add or remove elements from the UCM security domain 249
- VxWorks systems and devices 251
- Co-resident Call Server and Signaling Server systems 252
- Join a Co-resident Signaling Server to the UCM security domain using Base Manager 253
- Redundant systems 266

Move an element from one UCM security domain to another 267
- Moving a Linux member element to another UCM security domain 267
- Moving a single VxWorks element to another UCM security domain 268
- Moving all VxWorks elements on a Call Server to another UCM security domain 269

Authentication methods 269

Central authentication 270
Secure UserID and password authentication with a system security token 271
Regenerate the Secure FTP Token 272
Refresh system keys 272
Control access to system Application Processors 273
Configure Secure File Transfer Protocol 274
sFTP configuration using overlays 274
sFTP configuration using Element Manger 276
Configure port access restrictions 277
Port Access Restrictions configuration page 277
Backing up and restoring port access restrictions 279
System wide administration commands in LD 117 279
Configure port access restrictions using Element Manager 280
Configure remote access 286
Manage secure shell access from the Call Server using overlays 287
Manage insecure shell access from the Call Server using overlays 288
Manage insecure shell access on Signaling Server or Voice Gateway Media Card devices using CLI 288
Enable or disable shell access using Element Manager 289
Access the system remotely 290
SSH key synchronization between active and inactive cores 291
Manage SSH keys using overlays 291
Manage SSH keys using CLI 294
SSH key management using Element Manager 296
Customize the logon banner 297
Manage the custom banner using overlays 297
Manage the custom logon banner using Element Manager 299
Force an EDD using overlays 301

Security debugging 303

Media Security debug tools 303
Enable or disable Media Security debug mode 303
View information about Media Security debug 305
Use Media Security Debug 306
IPsec debug tools 311

Security logs and alarms 315

Media Security OMs 315
Traffic measurement 315
Media Security OMs on Signaling Server 316
OAM Security OMs 317
Default password change warning 317
Warning message for Force Password Change 317
TLS logs and alarms 317
sFTP security alarms 319

OAM Transaction Audit and Security Event logging 319
- Security Event log 319

A: Standards **321**

Media Security FIPS conformance 321
Encryption technology 322
Encryption technology supported in UNIStim DTLS 322

New in this release

The following changes are introduced in *Security Management Fundamentals* (NN43001-604) for Nortel Communication Server 1000 Release 6.0:

> **ATTENTION**
> The Enterprise Common Manager (ECM) framework is now referred to as Nortel Unified Communications Management Common Services (UCM Common Services).
>
> When referring to applications deployed from within UCM Common Services, the term Unified Communications Management (UCM) is used.

- Centralized authentication and policy management through UCM Common Security Services
- Enhancements to Intrasystem Signaling Security Solution (ISSS)
- Enhancements to secure file transport
- Improved hardening capabilities for Linux and VxWorks platforms
- DTLS encryption for improved signaling security
- Enhancements to Secure Real time Transfer Protocol (SRTP) and TLS for Microsoft and UCM interoperability

Other changes

See the following sections for information about changes that are not feature-related.

Revision history

April 2010
Standard 03.08. This document is up-issued to correct the audit service default value to disabled.

March 2010
Standard 03.07. This document is up-issued to support Communication Server 1000 Release 6.0, and to add information about Datagram Transport Layer Security (DTLS).

March 2010
Standard 03.06. This document is up-issued to support Communication Server 1000 Release 6.0.

January 2010
Standard 03.05. This document is up-issued to support Communications Server 1000 Release 6.0.

June 2009
Standard 03.04. This document is up-issued to support Communications Server 1000 Release 6.0. The section on ISSS configuration has been updated.

June 2009
Standard 03.03. This document is up-issued to support Communications Server 1000 Release 6.0.

May 2009
Standard 03.02. This document is up-issued to support Communications Server 1000 Release 6.0.

May 2009
Standard 03.01. This document is up-issued to support Communications Server 1000 Release 6.0.

April 2008
Standard 02.08. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5, and to add support for UNIStim 3.0.

April 2008
Standard 02.07. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5, and to add information about Media Security and SIP Phones.

March 2008
Standard 02.06. This document is up-issued to support CS 1000 Release 5.5, and to add information about Mobile Extensions.

January 2008
Standard 02.05. This document is up-issued to support CS 1000 Release 5.5.

December 2007
Standard 02.01 This document is up-issued to support CS 1000 Release 5.5.

October 2007
Standard 01.46. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related to password reset procedures.

October 2007
Standard 01.42 This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related to Intrasystem Signaling Security Solution (ISSS) configuration.

September 2007
Standard 01.34 This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related primarily to ISSS configuration.

June 2007
Standard 01.13. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about SIP TLS and ISSS configuration.

May 2007
Standard 01.06. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about SIP TLS configuration, and corrections to statements about password conversion.

May 2007
Standard 01.03. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about Media Security configuration.

May 2007
Standard 01.02. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to NKEY configuration ranges.

May 2007
Standard 01.01. This document is issued to support CS 1000 Release 5.0 This document contains information about security features that are new in CS 1000 Release 5.0, and about changes to existing security features. This document also contains information previously contained in the following legacy document, now retired: *System Security Management* (553-3001-302).

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 chapter provides an overview of the document. The chapter is divided into the following sections:

- “Purpose” (page 17)
- “Navigation” (page 18)
- “About this document” (page 19)

Purpose

This document contains the information you need to secure your Communication Server 1000 (CS 1000) system using UCM Common Services, including:

- how to create and control OAM and PDT accounts
- how to protect configuration and application data
- how to protect signaling and the media stream from privacy intrusions or disruption
- how to administer and use secure remote access for OAM and PDT CLI, as well as secure Web access to Linux base through HTTPS and other secure protocols

This document contains information about configuring security features using Unified Communications Management (UCM), overlays, Element Manager, and command line interfaces (CLI).

For information about Unified Communications Management, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

For information about preventing misuse of system resources, such as unauthorized long distance calling, see *Telephony Services Access Control Management* (NN43001-602).

Navigation

This document includes the following chapters:

- “Introduction” (page 17)
- “Recommended security practices” (page 51)
- “Fundamentals of system security management” (page 21)
- “ISSS” (page 69)
- “Certificate Management” (page 95)
- “SIP security” (page 169)
- “Media Security” (page 183)
- “User and password management” (page 209)
- “Security administration” (page 247)
- “Security debugging” (page 303)
- “Security logs and alarms” (page 315)
- “A: Standards” (page 321)
- “Terminology” (page 325)

Other security information

This Nortel Technical Publication (NTP) provides information about many of the features you can use to provide security for your Communication Server 1000 system. Some security features are described in other NTPs. For more information, see Table 1 "Other NTPs that contain security information" (page 18).

Table 1
Other NTPs that contain security information

Telephony Services Access Control Management (NN43001-602)
Element Manager System Reference — Administration (NN43001-632)
Unified Communications Management Common Services Fundamentals (NN43001-116)
IP Phones Fundamentals (NN43001-368)
Secure Multimedia Controller Fundamentals (NN43001-325)
Network Routing Service Fundamentals (NN43001-130)
Linux Platform Base and Applications Installation and Commissioning (NN43001-315)

About this document

This document provides an overview of how you can control unauthorized access and provide security for the system. It describes reasons for implementing system security and provides recommendations for preventing abuse and damage to the telecommunications facilities.

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 6.0 software and UCM Common Services. For more information on legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page: www.nortel.com.

The subject of this document is the implementation of system-wide security features.

Applicable systems

This document applies to the following systems:

- Communication Server 1000E (CS 1000E) CP PIV and CP PM
- Communication Server 1000M Single Group (CS 1000M SG) CP PIV
- Communication Server 1000M Multi Group (CS 1000M MG) CP PIV
- Meridian 1 PBX 61C CP PIV
- Meridian 1 PBX 81C CP PIV

Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 software and configured to include a Signaling Server, they become CS 1000 systems.Table 2 "Meridian 1 systems to CS 1000 systems" (page 19) lists each Meridian 1 system that supports an upgrade path to a CS 1000 system.

Table 2
Meridian 1 systems to CS 1000 systems

This Meridian 1 system...	Maps to this CS 1000 system
Meridian 1 PBX 11C Chassis	CS 1000E
Meridian 1 PBX 11C Cabinet	CS 1000E

This Meridian 1 system...	Maps to this CS 1000 system
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

Intended audience

This document is intended for security solution designers, technical support personnel, and administrators responsible for configuring and managing security features.

Terminology conventions

In this document, the following systems are referred to generically as "system":

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

Fundamentals of system security management

This chapter provides an overview of the security options in the Communication Server 1000 system. The chapter is divided into the following sections:

- “System security overview” (page 23)
- “General signaling security overview” (page 23)
- “Platform security overview” (page 28)
- “Internal communications security overview” (page 36)
- “Media and signaling security overview” (page 42)
- “User and password management concepts” (page 45)
- “Security administration concepts” (page 49)

To protect voice media and signaling during transmission, you must complete all of the following steps:

- Configure Intrasystem Signaling Security Solution (ISSS) to protect IP traffic on the system.
- Configure SIP TLS to protect signaling traffic.
- Configure Media Security to encrypt the call stream.

ISSS protects communications over the Communication Server 1000 system elements Embedded LAN (ELAN) interface and Telephony Services LAN (TLAN) interfaces.

ATTENTION
In a campus redundancy configuration, ISSS/IPsec does not secure the high-speed pipe between Call Server 0 and Call Server 1.

Communication Server 1000 Release 6.0 includes several system components, including a Call Server, Signaling Servers, Co-resident Call and Signaling Servers, Voice Gateway Media Cards, and Media Gateways. The following list describes devices that connect through ELAN, and the devices that connect through TLAN:

- Most ELAN subnet communication is protected by ISSS/IPsec. The following components connect through their ELAN interfaces to the ELAN subnet, where communication is protected by ISSS:
  - Element Manager ELAN interface
  - CP Side 0 and CP Side 1 of the CS 1000 logical Call Server (LCS) with the high availability option
  - Co-resident Call Server and Signaling Server
  - Signaling Servers associated with a specific Call Server
  - Voice Gateway Media Cards (VGMC) and Media Gateway Controllers (MGC) in collocated IP Media Gateways (IPMG)

  All systems include an ELAN subnet to which the Communication Server 1000 Call Server ELAN interface and its collocated system elements connect. The MGC and its media daughterboard exchange control information using their ELAN interface.
- Some ELAN subnet communications are not protected by ISSS/IPsec. Contact Center and Call Pilot connect through their ELAN interfaces to the ELAN subnet, but their communication over the ELAN subnet is **not** protected by ISSS when ISSS is configured at Optimized security level. Communication is protected by IPsec when ISSS is configured at Full security level.
- Communication through the TLAN subnet is not protected by ISSS/IPsec. The exception to this rule is the AML communications link when the AML Front End application is deployed on a Signaling Server, in which case the AML link on the TLAN can be protected by ISSS. The following are examples of components that connect through their TLAN interfaces to the TLAN subnet:
  - Element Manager TLAN interface
  - Signaling Servers associated with Alternate Call Server for remote survivable MG 1000E IP Media Gateways (IPMG)
  - Geographic Redundancy Alternate Call Servers for remote survivable MG 1000E IPMGs
  - MGC media daughterboard
  - Voice Gateway Media Cards in IPMGs
  - Collocated IPMG Media Gateway Controllers (MGC)

In addition to Communication Server 1000 system components, Communication Server 1000 supports Linux-based Network Routing Service (NRS). NRS can run on any Linux servers anywhere within an Enterprise network, even sites that are geographically remote from Communication Server 1000 system components.

System security overview

The Communication Server 1000 system has a common security policy for voice and data networks that includes the following security functions:

- Platform security
  - Linux security hardening
  - Signaling encryption, which prevents theft of service, spoofing, and Denial of Service (DoS)
  - System hardware and software is designed to provide hardening and protection against Denial of Service (DoS) attacks
- Security management
  - Central authentication
  - Strong password management
  - Web-based management that is secured by Secure Sockets Layer (SSL)
  - CLI-based management that is secured by SSH
  - Security logs and alarms provide accountability and notification
  - Secure billing records protects confidentiality, theft of service
- Voice Media Security
  - Signaling and Media encryption ensures voice confidentiality and privacy
  - Client Authentication controls access to services

General signaling security overview

This section provides an overview of key management concepts and public-key certificate concepts.

Key management concepts

The encryption technology used in Communication Server 1000 relies on cryptographic keys that the system uses to encrypt information prior to transmitting it, and subsequently decrypt the information after it is received.

Key generation

The strength of an encryption system depends on two factors:

- the strength of the encryption algorithm
- the strength of cryptographic keys

Communication Server 1000 uses an industry-standard encryption algorithm, so cryptographic keys are the only factor that determine the security of encryption on the system. To this end, cryptographic keys used by Communication Server 1000 are random and very difficult to predict.

To further enhance the security of cryptographic keys, new keys can be generated periodically. In some instances on the Communication Server 1000 system, these new keys are generated automatically; in others, you must periodically refresh the keys manually.

Key exchange

Secret keys can be shared between two endpoints in one of the following ways:

- distributed to the individual endpoints by a central server. This method requires that the distribution itself be secured to reduce the risk of corruption or interception of the keys. Media Security keys and ISSS preshared keys are shared using this method.
- preshared between endpoints in the system. You can manually configure preshared keys used by some features. Pre-shared keys for manually added ISSS targets are shared using this method.
- exchanged using a certificate with public-private key pairs. The certificate of the server is sent in the initial handshake. The public key of the server is used to encrypt a random session key, and the random session key is then transmitted. The server then uses the unique private key to decrypt the generated session key, and thereby obtain a unique shared session key which is used by both sides during the life of the session. Element Manager, Unified Communications Management, DTLS, and SIP TLS keys are exchanged using this method. The certificate contains a digital signature that verifies the identity of the owner of the public key in the certificate. Certificates are either self-signed, or signed by a CA:
  - — Some features can use certificates that are self-signed, but self-signed certificates do not provide authentication and is not scalable.
  - — Certificates issued by a local private CA or a public CA use Public Key Infrastructure (PKI). Third-party signed certificates can usually provide authentication, and are scalable.

For more information about public-key certificates, see "Public-key certificate concepts" (page 25).

Public-key certificate concepts

Overview

SSL, TLS, and DTLS protocols are used to provide transportation layer security for web-based HTTP management traffic, UNIStim, and SIP signaling traffic between NRS and SIP gateways. Using techniques based on public-key encryption, SSL/TLS provide entity and message authentication and communication privacy to upper layer applications and allow them to communication across networks in a secure manner. SSL/TLS can prevent eavesdropping, replaying attacks, and message tampering and forgery. You can also use TLS to protect SIP signaling between SIP Phones and the SIP Line Gateway.

An SSL/TLS connection involves two parties: a client and a server. The client initiates the connection, and the server responds to the connection request. An SSL/TLS server must have an X.509 certificate which it sends to the client to be verified during SSL/TLS handshaking. The server X.509 certificate is usually digitally signed by a Certificate Authority (CA). An SSL/TLS client authenticates the server X.509 certificate by performing a series of validations, including:

- validating the CA digital signature on the certificate using the signing CA public key
- verifying that the signing CA public key certificate is on the client's trusted certificate list
- verifying that the server certificate is not expired or revoked
- verifying that the FQDN and the IP of the connection is consistent

The certificate chain is a series of certificates provided by the CA issuing the certificates to the endpoints. The certificate chain begins with the peer certificate and completes with the root certificate of the hierarchy. Each certificate is signed with the private key of the issuer, which can be verified with the public key of the next certificate in the chain. To be successfully imported into the Signaling server using Unified Communications Management, the certificates must be compiled into a single PEM file.

Certificate management

SSL/TLS for protecting HTTP management traffic supports only server side certificate-based authentication. TLS for SIP supports both server side and client side certificate-based authentication (mutual authentication). DTLS-capable IP Phones can validate certificates on the Signaling Servers and Media Cards.

Unified Communications Manager provides a centralized console for managing X.509 certificates, including issuing certificates, distributing certificates to Communication Server 1000 devices (for example, a SIP Gateway), revoking certificates, and managing the trusted CA certificate list on Communication Server 1000 devices.

For example, from the certificate management console, X.509 certificates can be assigned remotely to Web SSL and SIP TLS services on SIP Gateways, as well as NRS and Element Manager servers. Different services on the same device can have their own certificates, such as DTLS, or share a common certificate. For example, Web SSL and SIP TLS services that are active on the same device can share the same X.509 certificate.

Certificate types

The Unified Communications Management certificate management console supports the following types of certificates:

- **Self-signed certificates.** Self-signed certificates are not issued by a CA. This type of certificate does not provide secure authentication and is vulnerable to third-party intercepts. Nortel recommends that you avoid using self-signed certificates whenever possible.
- **Certificates signed by the private CA hosted on UCM primary security server.** During the installation of the Unified Communications Management primary security server, a private CA is created. You can use the private CA to issue certificates to remote devices in the same security domain. When a certificate is issued from Unified Communications Management primary security server and distributed to a remote device, the root certificate of the private CA is automatically added to the trusted certificate list on that device. As a result, devices that use certificates issued by the same private CA always trust each other.
- **Certificates signed by a public CA**. A public CA can be an existing internal CA from within your organization or an outside commercial CA (such as Verisign or Thawte). You can use the Unified Communications Management X.509 certificate management console to generate a Certificate Signing Request (CSR) from a target device and transfer it to a public CA for a certificate response containing an X.509 certificate. You can then use the Unified Communications Management certificate management console to process the certificate response returned from a public CA and distribute the X.509 certificate to the target device.

Trusted certificates list

To establish mutual trust between two SIP TLS endpoints using certificates signed by a public CA, the TLS client and server must add each other’s signing CA certificate to their trusted CA certificate lists using the Unified Communications Management certificate management console.

If a public CA is hierarchical, consisting of a root CA and one or more intermediate CAs, add both the root CA certificate and all intermediate CA certificates to the trusted certificate list of a device. However, if you use a certificate signed by either Verisign or Thawte for your SIP Gateway, add the root CA certificate to the SIP Gateway’s trusted certificate list, but do not add the intermediate CA certificates.

Third-party CAs and chains of trust

Third-party CAs are used to verify the identity of the owner of a certificate by referring a series of certificates, each one verifying that the next item in the sequence can be trusted, until a trusted public CA (the root) is reached. This sequence of verification is sometimes referred to as a chain of trust.

When a certificate is presented to the SIP Proxy, the SIP Proxy verifies the same number of CAs as is in the chain of trust. On the SIP Proxy, the number of CA trust certificates installed must be the same as the number of certificates in the chain. However, on a SIP Gateway, you only need to install the intermediate CA to the trust list for Verisign and Thawte.

Table 3 "Examples of certificates in a chain" (page 27) shows examples of the certificates included in a chain.

Table 3
Examples of certificates in a chain

Certificate source	Certificates included
Certificate built by Intermediate	Certificate, Intermediate, and Root CA
Certificate built off root	Certificate and Root CA

Unified Communications Management does not use an intermediate CA to sign a certificate. Instead, it uses a self-signed private root certificate. For Verisign or Thawte certificates, you must import the root certificate and intermediate certificate for a SIP Proxy, but only the intermediate CA certificate for a SIP Gateway.

Before installing a certificate signed by a third-party vendor other than Verisign or Thawte, consult Nortel technical support. For certificates signed by some third-party vendors, you must import root certificates and intermediate certificates on both the SIP Proxy and SIP Gateway.

To use certificates signed by a third-party CA, you must complete the following steps:

- Configure the certificate request.
- Obtain the certificate from a third-party CA.
- Process and install the certificate signed by the third-party CA.
- Add the CA to an endpoint.

Certificate management and SSL/TLS configuration

You can use Unified Communications Management to manage certificates for Web SSL, DTLS, and SSL/TLS endpoints. Use the certificate management tools provided by Unified Communications Management to import, export, revoke, and assign certificates and to create certificates or certificates requests.

To manage certificates using Unified Communications Management, you must have Security Administrator access.

For certificate and CA management procedures, see “Certificate Management” (page 95).

Platform security overview

This section provides an overview of platform security features.

Unified Communications Management security services

Nortel Unified Communications Management (UCM) Common Services framework is an integrated and unified Web-based management interface for managing Call Servers, Application Servers, and the Converged Data Network. It is installed as part of the Linux base operating system.

The Unified Communications Management security services provide a centralized GUI-based interface for individual account administration for the entire Communication Server 1000 network. It is the primary interface for system-wide security configuration and administration and provides centralized authentication for users, systems, and devices by acting as a RADIUS server, providing authentication for RADIUS clients based on predefined roles and policies.

For information about Unified Communications Management authentication methods, see “Authentication methods” (page 269).

For information about Unified Communications Management Common Services, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Unified Communications Management security server roles

This section provides an overview of the Unified Communications Management security server roles. For details regarding the concepts described in this section, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Primary security server role

The primary security server stores all administrator identities, authorization data, and security configuration data. The server acts as a centralized location for authentication, authorization, and logging. Each network has only one primary security server.

The primary security server serves two roles, regardless of high availability options:

- The primary security server manages the Private Certificate Authority. It issues certificates for new member servers and is the only server from which the certificate management console can be used.
- The primary security server has write access to all security related data. All Unified Communications Management operations must be performed on the primary security server.

The primary security server contains, as part of its installation, the primary security repository, and is the server that administrators must use for configuring and managing Unified Communications Management.

A primary server cannot be demoted to a backup or member security role server.

Backup security server role

A backup security server exists to serve authentication and authorization requests when the primary server is unavailable. A backup server is optional, and any server may be designated the backup security server. There is only 1 backup security server on a network. You can access the backup server by typing the following URL into a browser: http://<FQDN_backup_server>.

In the event the primary server is unavailable, the backup security server performs the following:

- Manages all authentication and authorization requests; however, although you can still view the Unified Communications Management web pages, no changes can be made to the configuration options.
- Certificates continue to function normally; however, the certificate management pages cannot be viewed or modified.

As part of its installation, the backup server contains a read-only backup security repository. Backup servers always maintain real-time synchronization with the primary server.

Session failover is not supported. If a user is logged on to the primary server when it becomes unavailable, the user must log on again to the backup server.

The backup server login page displays a message that it is a backup server. The Navigator page on the backup server only shows Elements, Active Session, and Logs. While the user can view the elements table, no configuration changes can be made.

A backup security server cannot be promoted to a primary security server role.

Member security server role

A member server is a part of the secured network, but is not a primary or backup security server. A member server must send all security requests to the primary security server. Member servers do not have any Unified Communications Management web pages available and LDAP server is not active on it. Member servers only contain local login pages that are used for emergency situations.

When an administrator types the URL of the member server, the member server verifies that the primary is active. If the primary is active, then the user is forwarded to the primary server. If the primary is not active, then the user is forwarded to the backup security server. If the backup is also unavailable, then the user is forwarded to the local login page of the member server.

Session failover is not supported. If a user is logged on to the primary server when it becomes unavailable, the user must log on again to the backup server.

Security Domain Manager concepts

This section describes concepts associated with the Security Domain Manager (SDM). The SDM for VxWorks controls the joining of devices to security domain of the Unified Communications Management primary security server. Registering with the UCM security domain establishes mutual trust between the UCM primary security server and all other elements in the security domain. This enables system operations and communications to function normally. Elements that are not members of the security domain are non-trusted and will experience limitations in features that require secure communications to trusted elements, such as file transfer. Therefore, to ensure proper system operability and security, all elements in a system must be members of the same UCM security domain.

When a device joins the Unified Communications Management security domain, mutual trust is established between the device and the UCM primary security server. Once mutual trust has been established for the first time, the Unified Communications Management primary security server can send SSH remote commands or Secure FTP (sFTP) transfers to the device using RSA public key-based authentication.

> ***Note:*** sFTP must be enabled on the system for elements to join the security domain.

For the full list of commands for adding or removing elements from the UCM security domain, see “Add or remove elements from the UCM security domain” (page 249).

Linux security hardening

Linux security hardening is divided into the following two categories:

- Basic hardening
- Enhanced hardening

During the Linux base installation, the generic Linux base components are installed, then the basic and enhanced hardening items are applied. The enhanced hardening items are set to their default values when they are applied during the installation process. Hardening commands are only available for users with security administrator privileges.

When a Linux base upgrade takes place, the generic Linux base components are installed, then the basic hardening and enhanced hardening items are applied. If backed up data exists for the enhanced hardening items, then the values from the backed up data are used. If there are no backup values for enhanced hardening the default values are used.

Basic hardening

Basic Linux security hardening includes all hardening items that do not affect the performance of Nortel applications. This includes items such as the securing of log file and system configuration permissions, network parameters, removal of insecure accounts, disabling of unused programs and services, and the logging of each system login attempt.

Basic hardening items are turned on by default and they are not configurable. Although Basic hardening items are turned on by default, there can be instances where you can reapply Basic hardening values.

For example, you can reapply Basic hardening after the installation of third-party applications to ensure that all Basic hardening items are in secure status. Use the CLI command **`harden basic`** to perform this task.

Basic hardening is automatically applied to the corresponding Basic hardening items when applications are installed or uninstalled.

Enhanced hardening

Enhanced hardening items include all hardening items that can affect Nortel applications performance, or hardening items that require configuration. Enhanced hardening items that do not affect Nortel applications performance are turned on by default, enhanced hardening items that affect performance are turned off by default. Enhanced hardening items are configurable using Command Line Interface (CLI) commands.

Table 4
Enhanced hardening default values

Enhanced hardening item	Default value	Description
Audit service	off	Audit service is disabled by default.
Core dumps files	on	Core files are enabled by default.
FTP service	on	FTP service is enabled by default.
Network diagnostics	off	Network diagnostics are disabled by default.
Password days parameters	off	Secure values are used by default for password days parameters.
Pre-login banners	on	All banners have a default value.
Rlogin	on	Rlogin is enabled by default. ***Note:*** Rlogin is not available until the Call Server application is installed on the server.
SSH filtration	off	The source filtration of SSH connections is turned off by default; SSH connections are permitted.
Telnet service	off	Telnet service is disabled by default.
TFTP service	on	TFTP service is enabled by default.

Note 1: As certain enhanced hardening items are disabled by default (such as audit) and certain insecure items are enabled by default (such as FTP), the system remains in unsecured mode if the values are not changed.

Note 2: Unified Communications Management has various user roles. You must have a user role of security administrator to use hardening commands.

- Apply basic hardening.
- Enable or disable source filtering for SSH connections, and modify the filtering list.

  Note: If you manipulate the SSH filter, ensure the IP and subnet values are correct. Incorrect IP and subnet values will cause you to lose connectivity. If connectivity is lost, you must reestablish your connection using the console. If you configure SSH filtration, ensure that all members of the security domain are in the filtration list.

- Modify the pre-login logon banner. Use the CLI command **`harden banner`** to perform this task. Text files are accepted as custom banners. For example, if you wanted the banner to display the current version of Linux base, you could add the macro ##BASE_VERSION##.
- Modify the variables related to password lifetime. Use the CLI command **`harden passwd_days`** to perform this task.
- Configure the core dumps creation process. Use the CLI command **`harden coredumps`** to perform this task.

  Note: When the **`harden coredumps off`** command is issued, a system restart is necessary for the command to take effect.

- Enable or disable the Linux Audit daemon. Use the CLI command **`harden audit on[off]`** to perform this task.

  Note: If audit logs are enabled, you must provide storage for audit data. The logs will take up space until auditing is turned off.

- Enable or disable Trivial File Transfer Protocol (TFTP) service. Use the CLI command **`harden tftp`** to perform this task.
- Enable or disable File Transfer Protocol (FTP) service. Use the CLI command **`harden ftp`** to perform this task.
- Enable or disable telnet service. Use the CLI command **`harden telnet`** to perform this task.

- Enable or disable network tools (ethereal/wireshark, tcpdump, tracepath, traceroute). Use the CLI command **`harden nettools`** to perform this task.

  > ***Note:*** To use network analysis tools, the tools must be enabled by the administrator.Packages tcpdump, ethereal and ethereal-gnome, and commands traceroute, traceroute6, tracepath and tracepath6 are disabled in Nortel Linux base CS 1000. To enable these packages and commands use the **`harden nettools on`** command.

- Retrieve the status of enhanced hardening options. Use the CLI command **`harden status`** to perform this task.

Table 5 "Linux base CLI harden commands" (page 34) lists the CLI hardening commands and their description.

Table 5
Linux base CLI harden commands

Command	Description
harden audit on	Apply hardening to Audit Daemon.
harden audit off	Remove hardening from Audit Daemon.
harden audit status	Display the status of the Linux Audit Daemon.
harden banners set/file	Modify the banner text. The banner text will be replaced by the content from the file.
harden banners status	Enable or disable the pre-login banners.
harden basic	Apply basic hardening changes. Ensures that the basic hardening items are in secure status.
harden coredumps status	Enable or disable the coredump service.
harden ftp on	Apply hardening to FTP service.
harden ftp off	Remove hardening from FTP service.
harden ftp status	Display if FTP service is turned on or off.
harden help	Display help information for using the command.
harden nettools status	Enable or disable the nettools service.
harden passwd_days off	Disable previously configured parameters.
harden passwd_days on	Enable previously configured parameters.
harden passwd_days set -max	Set the value of the PASS_MAX_DAYS parameter. The default value is 90.

Command	Description
harden passwd_days set -min	Set the value of the PASS_MIN_DAYS parameter. ***Note:*** This parameter must be set to a value > or = 1. The default value is 1.
harden passwd_days status	Provide the current value of the parameters from hardening storage.
harden rlogin on	Apply hardening to remote logins.
harden rlogin off	Remove hardening from remote logins.
harden rlogin status	Display if hardening for remote logins is on or off.
harden ssh_filter -allow add –subnet	Add a subnet to the allowed list.
harden ssh_filter -allow del	Delete a host IP 1 from the allowed list.
harden ssh_filter -allow del -IP	Delete a host IP from the corresponding (allow or deny) filtration list.
harden ssh_filter -allow del –subnet	Delete a subnet from the allowed list.
harden ssh_filter -deny add -IP	Add a host to the deny list.
harden ssh_filter -deny del -IP	Delete a host IP from the deny list.
harden ssh_filter -deny del <number>	Delete a host IP from the corresponding filtration list. Each host entity (per line) has logical ordinal number in XML file storage. <number> is this sequence number.
harden ssh_filter status	Display the list of the names of the hosts which are allowed to connect to Linux base by SSH.
harden status	Retrieve the status of Linux base Enhanced Hardening options.
harden telnet on	Apply hardening to telnet service.
harden telnet off	Remove hardening for telnet service.
harden telnet status	Display if telnet service is turned on or off.
harden tftp on	Apply hardening to TFTP service.
harden tftp off	Remove hardening for TFTP service.
harden tftp status	Display if TFTP service is turned on or off.

Virus protection

The Nortel CS 1000 version of the Linux operating system for the server has been hardened and all extraneous packages have been removed. As the CS 1000 servers are running real-time telecommunication applications, the use of a real-time virus monitoring software is not recommended to be installed on these systems.

The software applications installed on the CS 1000 servers are pre-scanned by Nortel before being distributed. To minimize the risk of introducing a virus, you should not install third party software on these servers.

Any non real-time virus scanner installed should be run during a maintenance window after the telecommunication applications have been stopped. The virus scanner software must be stopped prior to the telecommunication applications being restarted. The virus scanner used cannot leave any background monitoring applications or daemons running on the server. The virus scanner cannot modify any of the system files (also known as inoculation). Always set the process priority of any such non real time virus scanner to low.

BIOS setting and password protection

To secure the server, Nortel recommends the following:

- Disable boot from CD or DVD drive in the Basic Input Output System (BIOS).
- Add a BIOS password. For information about configuring BIOS passwords for COTS servers, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

  > ***Note:*** The CP PM BIOS does not support a password. You cannot add a BIOS password to a CP PM server.

- Add a boot loader password.

Removal of the Ctrl+Atl+Del keyboard shutdown command

The Ctrl+Alt+Del shutdown command is disabled.

Single-user-text-mode booting is disabled

This booting mode is disabled to prevent the unauthorized access of the system.

Internal communications security overview

ISSS/IPsec

ISSS provides an IP Security (IPsec) solution that works with all IP protocols. IPsec works at a low layer of the network (Layer 3 of the OSI 7-Layer Model). This makes it possible for software applications to engage in secure communications without the need to add additional communications security code to each application.

IPsec encrypts the data stream between the two endpoints of a connection. A preshared key (PSK) is used to authenticate the two endpoints, and an encryption key is negotiated by using IKE.

ISSS/IPsec is managed and configured using the Unified Communications Management ISSS interface. The settings are propagated throughout the system by the primary security server to all Unified Communications Management-registered targets.

Communication Server 1000 Release 6.0 includes several system components, including a Call Server, Signaling Servers, Voice Gateway Media Cards, Media Gateway Controllers and Element Managers. In certain configurations, these components can be co-resident on the same element, for example, a Signaling Server co-resident with a Call Server. Communications between these elements is primarily through the ELAN.

Communication between certain auxiliary systems (such as Call Pilot, Symposium Contact Center, or Telephony Manager) is normally through the ELAN interface on the Communication Server 1000 elements; however, in the case of the AML protocol, communication may also occur through the TLAN interface.

ATTENTION
Previous versions of ISSS/IPsec are not supported in Communication Server 1000 Release 6.0. When a Communication Server 1000 system is upgraded to Release 6.0, IPsec must be reconfigured using the ISSS interface on the Unified Communications Management primary security server.

In addition to Communication Server 1000 system components, Communication 1000 supports the UCM primary and backup security server and Network Routing Service (NRS) elements. Although these elements can be configured to be co-resident with elements of a particular Communication Server 1000 system component, they are not specifically protected by ISSS/IPsec because they communicate using application secured protocols or through their TLAN interfaces.

You can enable ISSS at two levels, Optimized and Full.

- Optimized level provides basic protection, securing two key internal protocols on the ELAN interface and restricting access to these protocols to only trusted members of the UCM Security Domain.
- Full level provides protection for all protocols that are not secured at the application level (such as SSH, LDAPS, HTTPs, BOOTP, and RADIUS) on the ELAN interface. Protection is also provided for the AML protocol on the TLAN interface of Linux-based elements. Access to the protected protocols is restricted to only trusted members of the UCM security domain.

Security for the TLAN interface is provided by the Port Access Restrictions and Master Firewall Control features and platform hardening features.

For procedures relating to ISSS/IPsec, see “ISSS” (page 69).

Secure File Transfer Protocol concepts

Secure Shell (SSH) Secure File Transfer Protocol (sFTP) is installed and enabled on Communication Server 1000 Release 6.0 systems by default. This secure protocol replaces regular File Transfer Protocol (FTP) and other insecure data transfer protocols for several Communication Server 1000 applications. A list of applications using sFTP and FTP is shown in “Applications using sFTP and FTP” (page 40).

sFTP allows data to be securely transferred between an sFTP client and server over an encrypted and authenticated secure channel. In addition, sFTP allows a client and a server to authenticate each other by using a password. Devices obtain authentication and access control permissions for CLI access from the Unified Communications Management primary security server. Remote Authentication Dial In User Service (RADIUS) parameters are sent from the Unified Communications Management primary security server to the Call Server using SSH protocol. sFTP uses port 22, which is the same port used by SSH.

The authentication process for internal transfers uses the UCM security token as part of the authorization process. All elements using sFTP for internal transfers must have the same security token as distributed and synchronized by the UCM primary security server.

Not all Communication Server 1000 applications are compatible with sFTP. To provide backward compatibility for those features that are not compatible with sFTP, conventional FTP is still used for file transfer sessions between Release 6.0 systems and systems with previous versions. For systems and applications that are not compatible with sFTP, IPsec protocols are used for security.

To prevent incoming connections from using a high amount of system resources for extended periods of time, you can configure an sFTP session timeout using the LOUT parameter in LD 17.

The following characteristics apply to sFTP:

- The public key of a sFTP server is always trusted by sFTP clients, so there is no requirement for verification.
- ISSS security for specific elements can be disabled using the UCM primary security server. When disabled, all communications from the specified IP address of the element are sent without IPsec to protect the messaging traffic to the other elements of the Communication

Server 1000 system. Manual targets with ISSS disabled must be configured without IPsec; communications between other elements is not affected.

- A user name and password is used by a sFTP server to authenticate a sFTP client (public key-based authentication is not supported for authenticating a sFTP client). For internal automated transfers, the UCM security token is used to construct the password.
- TFTP for transferring tone and cadence files is not changed
- Not all FTP applications use sFTP; some will continue using standard FTP
- Interactive users of sFTP have restricted directory access.

For commands and procedures related to the concepts described in this section, see “Configure Secure File Transfer Protocol” (page 274).

sFTP for Linux platforms

sFTP for Linux is provided by the integrated openSSH functionality that is part of the Linux base operating system.

File transfer options for Linux and VxWorks platforms

Table 6 "File transfer options for Linux and VxWorks platforms" (page 39) shows the various file transfer options available for Linux and VxWorks platforms.

Table 6
File transfer options for Linux and VxWorks platforms

	Linux			**VxWorks**		
Method	**FTP**	**sFTP**	**TFTP**	**FTP**	**sFTP**	**TFTP**
Default	ON	ON	ON	ON	ON	ON
Options	OFF/ON$_1$	ON	OFF/ON $_1$	OFF/ON $_2$	OFF/ON $_3$	ON
$_1$ with Linux harden command						
$_2$ with Disable/Enable Transfer Insecure command						
$_3$ with Disable/Enable Transfer Secure command						

> ***Note:*** Nortel recommends that you do not disable secure transfers.

SSH client

The SSH client is implemented to facilitate access to an SSH server. There is no Command Line Interface (CLI) implementation of the SSH client for VxWorks platforms; however, there is access to the SSH client on Linux hosts. The joinSecDomain/REGISTER UCMSECURITY [DEVICE/SYSTEM] command, used for joining the

Unified Communications Management security domain, uses the SSH client to communicate with the Unified Communications Management primary server but does not provide any shell level access.

The Communication Server 1000 Release 6.0 system supports unsecured remote access methods, such as rlogin and telnet, but you can disable them.

Applications using sFTP and FTP

In Communication Server 1000 Release 6.0 and later, Secure File Transfer Protocol (sFTP) is used for most file transfer operations, with the following exceptions where File Transfer Protocol (FTP) continues to be used:

- File Transfer Protocol (FTP) is used to transfer database backups from the Communication Server 1000 Call Server to an external backup server. You can secure this transfer by configuring ISSS at the FULL level.
- FTP is used by Survivable Remote Gateway (SRG) to obtain IP client firmware from the Line TPS applications on Signaling Server elements. You must enable secure transfer on these elements.
- FTP is used to transfer files between Telephony Manager (TM) and the Communication Server 1000 Call Server. You can secure this by configuring ISSS at the FULL level.
- FTP is used when upgrading Media Gateway Controllers (MGC) and Media Cards (MC32, MC32S) from Release 5.x to Release 6.0. This requires that secure transfers be enabled on the Call Server (MGC) and Signaling Server (MC32, MC32S).
- If insecure transfers are enabled, third party applications or interactive users can use FTP for transferring files to and from Communication Server 1000 elements. sFTP is recommended for these transfers.

  Note: There is no impact during an upgrade to Release 6.0 even if CallPilot or Telephony Manager (TM) is part the system. CallPilot or TM normally functions as a client, so they can continue to use an FTP client to communicate with a Release 6.0 Call Server that supports both sFTP and FTP server.

Port access restrictions concepts

You can use port access restrictions to prevent port-based attacks on VxWorks-based system components by configuring port access rules. These rules are installed during initial Communication Server 1000 Release 6.0 software installation and are preconfigured with default settings. The port access restrictions feature is off after installation.

ATTENTION
There may be an interaction with ISSS/IPsec as the port access restrictions feature provides the ability to block specific ports. For example, if port access restrictions is configured to block TCP port 123 (NTP), IPsec encrypted traffic can still bypass the firewall over TCP port 123 as IPsec uses the Encapsulating Security Payload (ESP) protocol to encapsulate and transmit data.

The port access restrictions only filter inbound traffic for TCP and UDP port-based protocols. The port access rules completely protect the ELAN interface for the Call Server, MGC, and MC32S, and part of the TLAN interface for MGC and MC32S (non-call related traffic on the TLAN for MGC and MC32S is blocked).

> ***Note:*** The Co-resident Call Server and Signaling Server runs on Linux and is protected by the Linux firewall. You cannot configure the port access restrictions rules for this type of Call Server itself, but you can configure the port access restrictions for its MGC and MC32S cards.

The port access restrictions rules can be in one of three states: off, default, or custom. The default rules are installed as part of installation and, if desired, users can choose to download and configure a custom rules file to replace the default rules with their own specific port blocking needs. A port access state indicating file indicates whether the feature is currently active or not. After ELAN links are established with its dependent devices, the Call Server passes the state to dependent VGMC platforms and the rules are automatically propagated from the Call Server to dependent VGMC platforms as required. This ensures a matching state between the Call Server and its dependent devices.

You can configure the port access rules using LD 117 or EM, but there are a few mandatory rules that cannot be modified or deactivated. The mandatory rules are considered system essential and remain in an activated state regardless of whether the port access is configured with default or customized settings. For information about mandatory ports, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

> ***Note:*** The Call Server component of this feature is directly related to the Call Server software release. If an upgrade is performed and the software is later backed out or downgraded, reinstalling a previous release will overwrite the access restrictions default and state files.

For procedures related to the concepts described in this section, see “Configure port access restrictions” (page 277).

Linux Master Firewall Control

The Master Firewall Control (MFC) is the Linux equivalent of the port access restrictions feature for VxWorks platforms.

Media and signaling security overview

When call security is not present, calls can be vulnerable to disruption or intrusions against privacy. A virtual private network (VPN gateway) is commonly used to secure voice and data traffic originating outside of the corporate network. However, a VPN gateway does not provide end-to-end security and can leave a large part of the network susceptible to malicious attacks by hackers.

For example, a VPN gateway cannot prevent an illegal Real-Time Transport Control Protocol (RTCP) BYE message from closing a Real-Time Protocol (RTP) stream prematurely, nor can it stop a malicious RTP packet from being injected into a conversation. Therefore cryptographic protection of media streams and the associated RTCP Control streams are available on the system.

You can protect the media stream using the Media Security feature, which provides Secure RTP (SRTP) protection, and protect UNIStim signaling commands by enabling DTLS encryption or by adding a Secure Multimedia Controller (SMC) 2450 to the system. SRTP is a secure extension of RTP, and can provide end-to-end encryption of the media stream, while UNIStim signaling security protects communications between UNIStim IP Phones and UNIStim servers.

Media Security concepts

The Media Security feature provides a means by which two endpoints capable of communication using Secure Real-Time Transport Protocol (SRTP) can engage in secure media exchanges. For procedures relating to Media Security, see “Media Security” (page 183).

Media Security protects the media stream between the IP Phone and the first IP termination, so Media Security can provide end-to-end encryption if the media stream passes over IP systems only. The Media Security feature provides end-to-end encryption of media exchanges between two supported IP Phones. For a list of IP Phones that support Media Security, see Table 7 "IP Phones capable of establishing a secure connection using Media Security" (page 42).

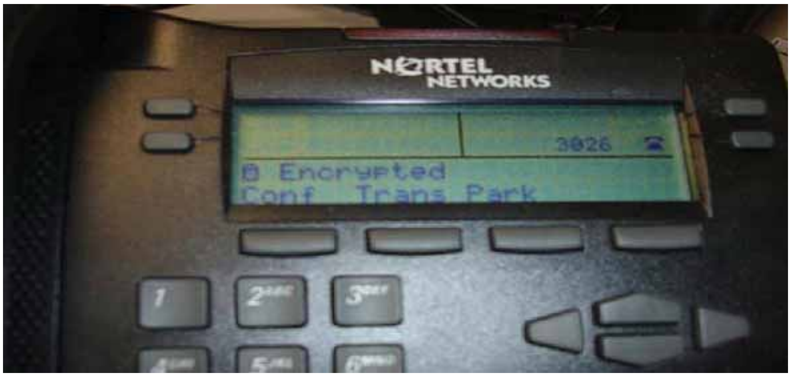
Table 7
IP Phones capable of establishing a secure connection using Media Security

IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E
IP Phone 2007
IP Softphone 2050
Phase II IP Phone 2001, Phase II IP Phone 2002, and Phase II IP Phone 2004

Security icon

If you enable Media Security, supported IP Phones use SRTP to encrypt and authenticate the media stream, and the system displays a security icon on the IP Phone to indicate that the media stream is encrypted. The icon is shown in Figure 1 "Security icon and text indicator on an IP Phone 2002" (page 43); on some phones, the message "encrypted" also appears. There is no visual indication on digital phones, analog phones, nonsecure IP Phones, or on IP Phones that have no display.

Figure 1
Security icon and text indicator on an IP Phone 2002



If you enable Media Security, end-to-end security is established for most calls, and the icon appears on both IP Phones whenever both of the following are true:

- Both IP Phones are capable of making a secure connection.
- Neither IP Phone has Media Security configured to Never.

The security icon indicates that the media stream is secured when it passes over IP systems. Calls that pass over non-IP systems cannot be secured by this feature.

Blocked call notification A call is blocked if, for example, one of the endpoints is configured to offer and accept only secure connections, but a secure connection cannot be established. When this occurs, no security icon appears, and overflow tone sounds for the originator of the call.

Dependencies and supported systems

Media Security is applicable to IP Phones, and is supported on all systems except TDM-only systems.

Media Security applies to the IP legs of a call and the Call Server sends the keys to the IP end points. These keys are transmitted over signaling links, therefore you must also protect signaling.

The security icon on an IP Phone indicates that the IP leg of the call is encrypted, but does not indicate whether or not the entire media path is protected.

TLS security for SIP trunks concepts

Transport Layer Security (TLS) is used to secure signaling between SIP endpoints. TLS provides message confidentiality and integrity, and it provides client-server authentication at the transport layer. For procedures relating to SIP TLS security, see "SIP security" (page 169).

TLS security operates on a hop-by-hop basis, so each segment of the call path must be secured individually. To ensure that calls are always secure, configure the system to always use TLS.

TLS protects communication between SIP endpoints by providing:

- Confidentiality: Symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret key negotiated through the TLS handshake protocol.
- Integrity: Message transport includes a message integrity check using a keyed message authentication code (MAC). Secure hash functions are used for MAC computations.
- Authentication: If certificates signed by a trusted certificate authority (CA) are used, the client in a TLS connection can authenticate the identity of the server, and the server can optionally authenticate the identity of the client.

UNIStim signaling encryption with DTLS

Secured UNIStim signaling encryption is provided by Datagram Transport Layer Security (DTLS). DTLS encrypts the data exchanges between the Signaling Server and the IP Phones. Previously, Secure Multimedia Controllers (SMC 2450) were required for UNIStim encryption, but DTLS requires no new additional hardware and can coexist with currently installed SMCs. DTLS and non-DTLS systems can be configured on the same network.

For information about how UNIStim with DTLS interacts with SMC 2450, see *Secure Multimedia Controller Fundamentals* (NN43001-325).

NRS SIP Proxy

SIP Proxy mediates between trusted and non-trusted SIP endpoints. For more information about SIP Proxy, see *Network Routing Service Fundamentals* (NN43001-130).

User and password management concepts

This section provides an overview of operations, administration, and maintenance (OAM) concepts, including information about account types, user and password management tools, and access control. For procedures relating to the concepts described in this section, see "User and password management" (page 209).

OAM overview

Users can use administration overlays to configure the customer database and conduct day-to-day routine system administration functions. Access to these overlays must be limited to only those users who require the use of them; unauthorized users can otherwise cause performance degradation or failure through misuse or malicious intent.

User accounts on the system fall into one of two categories: system default user accounts, and user accounts that you create. You can create user accounts and manage privileges using overlays, or using Element Manager.

> ***Note:*** Because the system reserves certain user names for system use, Nortel recommends that you do not create user accounts with naming formats such as NT_S_xxx, NT_xxx, and so on.

System accounts

Communication Server 1000 allows you to create user accounts for two modes of operation on the Call Server. The two modes of operation are:

- System operations, administration, and maintenance (OAM or PWD)
- Problem Determination Tool (PDT)

Each of these two modes provides two types of system account, which provide access to various database configuration and maintenance programs. The system supports up to 200 accounts, in any combination of the following types:

- PWD Level 1 user ID and password (PWD1)
- PWD Level 2 user ID and password (PWD2)
- PDT Level 1 user ID and password (PDT1)
- PDT Level 2 user ID and password (PDT2)
- Limited Access Password (LAPW)
- IP Phone Installer Password

Default user names and passwords are available for each of the two modes of operation, and are described in Table 8 "Default user names and passwords" (page 46).

Table 8
Default user names and passwords

	Password				
User Name	**Call Server**	**Signaling Server, Media Gateway Controller, Voice Gateway media Card**	**UCM**	**SMC 2450**	**NRS Manager**
ADMIN1 (also called PWD1 or default Level 1)	0000	Synchronized from the Call Server	na	na	na
ADMIN2 (also called PWD2 or default Level 2)	0000	Synchronized from the Call Server	na	na	na
PDT1 (also called PDT Level 1)	thorsgr8	Not applicable	na	na	na
PDT2 (also called PDT Level 2)	2tdp22ler	Synchronized from the Call Server	na	na	na
LAPW	Configured by the administrator	na	na	na	na
IP Phone Installer Password	na	na	na	na	na
admin	na	na	nortel12 _Nortel	admin	admin
oper	na	na	na	oper	na
boot	na	na	na	ForgetMe	na
root	na	na	na	ForgetMe	na

The Call Server Level 1 account (PWD1), Level 2 account (PWD2), and PDT Level 2 account (PDT2) become the system accounts for the Signaling Server and Voice Gateway Media Card. This change occurs when the Signaling Server and Voice Gateway Media Cards communicate directly with the Call Server and synchronize their passwords with the Call Server.

The capabilities of the Level 1 account (PWD1), Level 2 account (PWD2), and PDT Level 2 account (PDT2) accounts are described in Table 9 "Account level descriptions" (page 47).

Table 9
Account level descriptions

Account type	Description
PWD Level 1	You can use PWD Level 1 accounts to log on to the system to change the configuration database. Users that have Level 1 accounts cannot change passwords for Level 1 accounts, Level 2 accounts, or the secure data password associated with assigning Authorization Codes (Authcodes) and DISA parameters (if defined).
PWD Level 2	PWD Level 2 account provides all the privileges of Level 1 accounts. It also offers the option to enable Account Administration.
PDT1 Level 1	You can use accounts with PDT Level 1 privilege to access only PDT level 1 commands at the PDT prompt.
PDT Level 2	You can use accounts with PDT Level 2 privilege to access all PDT commands at the PDT prompt.
Limited Access Password (LAPW)	Use Limited Access to Overlays feature to create accounts that have limited access to overlays. LAPW accounts can be configured to require a user name of up to 11 alphanumeric characters. You can configure the user name using a PWD Level 2 account with the ability to administer accounts.

For more information about creating or changing passwords, see Table 40 "Job aid: LD 17 user and password prompts" (page 215). To display a list of all accounts that have insecure passwords, see Procedure 67 “Checking for insecure passwords using LD 22” (page 222).

ATTENTION
Passwords or account changes made on the Call Server are distributed or made permanent when you perform an Equipment data dump (EDD). Similarly, when you upgrade to Communication Server 1000 Release 6.0 or later, the system goes through account conversion. Account conversion is made permanent when you perform an EDD, at which time the accounts are distributed to all the attached devices.

Access control management

Unauthorized access to system programs (overlays) can leave the system vulnerable to misuse and performance degradation or failure. Use administration overlays to configure the customer database and conduct routine system administration, and to limit access to system resources. For more information about managing access control, see *Telephony Services Access Control Management* (NN43001-602).

System upgrade password conversion

In Communication Server 1000 Release 6.0, all passwords are hashed using SHA-256 and the hash values of passwords are stored in the system. The first time a user logs on after the system is upgraded to Communication Server 1000 Release 6.0 or later, the hash for that user's password is computed using SHA-256 and then stored.

Global password settings

The system offers the following security options for each password, which help to prevent unauthorized access:

- Force Password Change (FPC) prevents users from continuing to use the system default passwords.
- Failed Log In Threshold controls the number of times a user can fail to log on before the port they are using is locked. To override a lockout, manually restart the system.
  - Port lockout time after failed log in controls the length of time the port is locked after the Failed Log In Threshold value is reached.
- Password complexity check tests user passwords to verify that they are difficult to guess.
- Audit trail for password usage prevents the reuse of a password.
- Last Log In Identification keeps track of the last user who logged on.
- Inactivity timeout ends a logon session after a period of inactivity.

FPC is part of a feature called Default Password Change. This feature provides the following options:

- Warning message. A default password security warning message appears when users log on to a system where any of the system user names has a default password (PWD1, PWD2, PDT1, PDT2, and LAPW). The security warnings also appear if you change a system password from a nondefault value back to a default value.

  The system also generates a `SEC0029` message to record the event of the warning message.
- Force Password Change (FPC). Configure this feature to force a user who logs in using a default password to change the password before they can use the system.

Default Password Change does not apply to the IP Phone Installers passwords because IP Phone Installers passwords are assigned by a system administrator, and the system does not provide default values.

Role management in Unified Communications Management

Role management facilities are available on the system if Unified Communications Management is available. The role management facilities provide improved flexibility to control access to system resources and to change privileges for a user or group of users.

For example, you can assign individual access to the debugging shell (PDT) or change the access privileges of a group of users by modifying one of the roles assigned to them.

There are 6 predefined roles in Unified Communication Management:

- MemberRegistrar
- NetworkAdministrator
- Patcher
- CS1000_Admin1
- CS1000_Admin2
- CS1000_PDT2

For information about role-management and other security features available in Unified Communications Management, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Security administration concepts

This section provides an overview of the Secure Shell (SSH) protocol, and the customizable logon banner. For procedures relating to the concepts described in this section, see "Security administration" (page 247).

SSH and secure remote access

SSH provides a secure method to log on to a system remotely and perform system management operations. Using role definitions, you can grant specific users the ability to use SSH to connect to all parts of the system, or only to the parts you specify. This can include access to SL-1 on the Call Server, support for the CPSID user name and ptyxx user names, access to the Call Server PDT shells, the Voice Gateway Media Card shell, IPL shell, and the Signaling Server OAM shell.

SSH provides several authentication methods. Nortel recommends that you use the password authentication method.

Customizable logon banner

The system provides a customizable 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. You can use this feature to display up to 20 lines of custom text, with up to 80 characters on each line. The default text of the logon banner is shown in Table 10 "Default text of the customizable logon banner" (page 50).

Table 10
Default text of the customizable logon banner

The software and data stored on this system are the property of, or licensed to, Nortel Networks and are lawfully available only to authorized users for approved purposes. Unauthorized access to any software or data on this system is strictly prohibited and punishable under appropriate laws. If you are not an authorized user then log out immediately. This system may be monitored for operational purposes at any time.

You can configure the banner using Element Manager or LD 117 commands on the Call Server, which configures the banner used for the Call Server (if it is not a Co-resident system) and its dependent MGCs and VGMCs. For Co-resident Call Servers and other Linux platforms, you can configure banners for each element individually using the Linux base manager.

Recommended security practices

This chapter contains guidelines and describes settings and practices that Nortel recommends as best practices for securing your system. The recommendations in this section provide a starting point for configuring security on your system; you can have security needs that require different settings in some cases. The chapter is divided into the following sections:

- "Recommendations for OAM security" (page 51)
- "Recommendations to protect confidentiality" (page 53)
- "Recommendations for security administration " (page 54)
- "Security interactions" (page 58)
- "Recommendations for upgrading to Communication Server 1000 Release 6.0 from a previous release" (page 64)
- "Migrate existing CS 1000 Release 5.x user accounts to CS 1000 Release 6.0" (page 66)

For more information about the features described in this chapter, see "Fundamentals of system security management" (page 21).

Recommendations for OAM security

Nortel recommends that you implement the following operations, administration, and maintenance (OAM) security features:

- password management (see "User and password management" (page 209))
- Audit Trail review (see "Configure LAPW Audit Trail using overlays" (page 222))
- History File review (see "History File configuration using overlays" (page 233))
- Telephony Services Access Control management (see *Telephony Services Access Control Management* (NN43001-602))

Recommended password management practices

Poorly chosen passwords or insufficient password security practices can compromise system security. To maximize password security, Nortel recommends that you implement the following password practices:

- Change the default password after system installation and configuration.
- Change passwords every 60 to 290 days.
- Change the system password if anyone who knows the system password leaves the company.
- Do not reuse passwords.
- Use long passwords to provide greater security.
- Periodically change the IP Phone Installers passwords.
- Avoid simple passwords or those that are derived from personal information such as social security numbers, home telephone numbers, birth dates, and family names.
- Implement policies that prevent the use of system default passwords.
- Implement policies that prevent users from choosing simple passwords.
- Implement policies that discourage password guessing.

Upgrading user names from an earlier release

In Communication Server 1000 Release 6.0, user names are required for all log on sessions. If you upgrade from Communication Server 1000 Release 3.0, default user names are created for any users that did not have one in the past. The names that are created for these users are shown in Table 11 "User names created when accounts without user names are converted from CS 1000 Release 3.0" (page 53).

CAUTION

If you are upgrading from Communication Server 1000 Release 5.5 or earlier to Communication Server 1000 Release 6.0, Nortel recommends that you ensure that there are no PWD or LAPW accounts on the system that use the reserved names PDT1 or PDT2; if any exist, delete them and replace them with new accounts that have different user names. In Release 6.0, the system prevents you from creating accounts with these reserved names.

Table 11
User names created when accounts without user names are converted from CS 1000 Release 3.0

Account	User name
PDT1, PDT2, ADMIN1, ADMIN2	PDT1, PDT2, ADMIN1, ADMIN2
LAPW	USER0, USER1, USER2, USER3 If accounts are associated with the Limited Access Password (LAPW) users, the user names are preserved. If accounts are not associated with the LAPW users, names are automatically created (for example USER0, USER1). The order of naming is based on the order in which the users are listed prior to the upgrade. Nortel therefore recommends that you make note of the order in which the users are listed before commencing an upgrade.

Recommendations to protect confidentiality

To protect information during transmission, complete all of the following steps:

- Use DTLS-capable IP Phones.
- Configure Intrasystem Signaling Security Solution (ISSS) to protect IP traffic on the system.
- Configure Transport Layer Security (TLS) to protect Session Initialization Protocol (SIP) signaling traffic.
- Configure Media Security to encrypt the call stream.

ISSS/IPsec recommendations

Enable ISSS with at least the minimum setting (Optimized Security), to protect Embedded Local Area Network (ELAN) messages by enabling ISSS with at least the minimum setting (Optimized Security). You should not configure ISSS targets with ISSS disabled unless necessary as this exposes the system to possible attack from the IP address of the disabled target.

Preshared keys, SSH keys, and Secure FTP Token recommendations

The preshared keys (PSK) can be changed on UCM member servers on an infrequent basis; however, when changing SSH keys, you must rejoin the member to the UCM security domain.

It is not recommended to change the public/private SSH keys on the UCM primary security server. If you change the SSH keys on the UCM primary security server, you must rejoin all UCM member servers to the UCM security domain.

Periodic changing of the PSK and Secure FTP Token is recommended, but is not required on a frequent basis. In the event of a potential security breach, the PSK or Secure FTP Token can be changed as needed.

TLS security for SIP trunks recommendations

Protect the confidentiality of signaling on the SIP trunk using, for example, SIP TLS or a Virtual Private Network (VPN gateway). Nortel recommends configuring SIP TLS to the Best Effort policy, and selecting TLS as the Transport Protocol.

Media Security recommendations

Nortel recommends that you configure Media Security to use Best Effort (MSBT). This causes IP Phones to establish secure calls whenever possible, but to establish a connection without Media Security when a secure connection is not available. An icon on the IP Phone indicates when the call is secured using Media Security.

The keys that are used to encrypt voice streams are distributed using signaling (such as over SIP trunks or UNIStim) that do not secure the key material. Therefore, Media Security relies on the ISSS feature to protect the key material. Nortel recommends that you protect ELAN messages by enabling ISSS, protect UNIStim signaling by enabling DTLS, and protect signaling on the SIP trunk by enabling SIP TLS.

Recommendations for security administration

Secure Shell (SSH) provides several authentication methods; Nortel recommends that you use the password authentication method.

Shell Access Control

Upon installation or upgrade, Secure Shell (SSH) is enabled, but is unavailable while keys are being generated. Key generation takes two to three minutes on most systems.

Nortel recommends that you use SSH whenever possible, and disable insecure shells (rlogin, and telnet) on the Communication Server 1000 system, except as needed. Both Secure Shell and insecure shells are enabled by default. Table 12 "Examples of cases where insecure shells are required" (page 54) lists some instances where insecure shells are required.

Table 12
Examples of cases where insecure shells are required

Feature or device	Insecure shell required
Net IQ	If you plan to use Net IQ, you must enable insecure shells because Net IQ cannot use SSH.

Telephony Manager	If you plan to use Telephony Manager (TM), you must enable insecure shells because TM cannot use SSH.
MRV IR-8020	If your system includes an MRV IR-8020, you must enable insecure shells because that device requires rlogin.

If you must enable insecure shells, Nortel recommends using them only when required, and using SSH whenever possible.

Certificates

You can configure the Communication Server 1000 system to work with certificates provided by a certificate authority (CA), (which can be either a private certificate authority such as the Unified Communications Management certificate authority, or a public certificate authority such as Verisign or Thawte), or with certificates that are self-signed. Nortel recommends that you use a public or private CA and enable X509 authentication, because this option provides better authentication.

If the CA is not available, you can verify the identity of the Element Manager server by examining the fingerprints on the certificate. If a man-in-the-middle attack takes place, users can detect it because the fingerprints on the certificate do not match the Element Manager server.

SIP TLS certificates

Nortel recommends that you use the same type of certificates (private-CA, third-party, or self-signed) in all the systems involved in SIP TLS communication.

Third-party certificates

If you plan to use certificates signed by a public certificate authority for your SIP Proxy and Redirect server and SIP gateway, install both the root CA certificate and all intermediate CA certificates into the system. However, if you use certificates signed by either Verisign or Thawte, install only intermediate CA certificates into SIP gateway, but do not install the root CA certificate.

Security code for Mobile Extensions

If your system is configured to allow the use of Mobile Extensions, Nortel recommends that you require users to enter a security code in order to access the system using Mobile Extensions. For more information about configuring Mobile Extensions and security code restrictions, see *Features and Services Fundamentals Book 4 of 6 (I to M)* (NN43001-106).

Single sign-on cookie domain

If your system includes multiple domains and single sign-on does not work on your system, contact Nortel technical support.

Certificate management

Nortel recommends that you install your Element Manager on Unified Communications Management as the primary security server before you install your Linux-based NRS, and configure all of your NRS to be part of the same Unified Communications Management security domain.

Nortel recommends that you perform certificate management from the same Unified Communications Management Linux host that is running Element Manager, because you can then enable ISSS on all of the Communication Server 1000 system elements managed from that host. Element Manager on Unified Communications Management automatically associates ISSS with each system element every time you display the list of IP telephony nodes in the system (click on the appropriate link in Element Manager on Unified Communications Management). The system uses the same association to protect certificate management.

If you perform certificate management from an Unified Communications Management Linux host that runs Network Routing Services (NRS), Element Manager is not running, and you must manually associate ISSS with each system element managed by the system.

Certificate management across multiple UCM security domains

To simplify certificate management, Nortel recommends that you place all the NRS in a single top-level enterprise domain (a domain having the format xxxxx.yyy, for example nortel.com).

If you must place NRS in multiple top-level enterprise domains, Nortel recommends placing them in as few domains as possible. For more information, see Figure 9 "SIP TLS with multiple security domains" (page 170).

Upgrade from an earlier release

The following security administration issues pertain when you upgrade to Communication Server 1000 Release 6.0 from a previous release:

- In Communication Server 1000 Release 6.0, Unified Communications Management is the central framework for security configuration, authentication, and administration.
- Existing IPsec configurations must be reconfigured using the UCM ISSS configuration interface.
- SSH is enabled by default, but is not available until keys are generated. Keys are automatically generated, a process that takes less than three minutes on most systems, but can take up to two hours on TDM-only systems that use SSC as the call processor.
- CS 1000 Release 6.0 protects HTTPS through self-signed certificates. When you upgrade, new key pairs are generated for this certificate,

and are used for both TLS and HTTPS. Nortel recommends that you replace this with a new certificate signed by the primary security server.

- When you upgrade a SIP Gateway system from Communication Server 1000 Release 4.5 or later to Release 6.0 and plan to use a certificate signed by a public CA, Nortel recommends that you obtain the certificate before your upgrade. If you upgrade your SIP Gateway before obtaining the certificate, you will not have a certificate for immediate use after upgrading because it takes time to obtain the certificate.
  To obtain a certificate signed by a public CA, see Procedure 32 “Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading” (page 134), and Procedure 33 “Processing a pending certificate response for SIP TLS when upgrading” (page 138).
- When you upgrade a system to Communication Server 1000 Release 6.0, Secure File Transport Protocol (sFTP) is enabled by default.
- To enable DTLS encryption for UNIStim signals, the Communication Server 1000 system must be upgraded to Release 6.0 and the IP Phones must be DTLS-capable and have the latest firmware. Also, the system must be configured for at least Best Effort security level.

Recommendations to protect UNIStim IP Phones

The following recommendations pertain to steps you can take to secure UNIStim IP Phones connected to the system.

UNIStim with DTLS recommendations

On IP Phones that support it, Nortel recommends that you protect UNIStim signals with DTLS encryption. After Communication Server 1000 software installation (new or upgrade), DTLS signaling security is disabled by default (DTLS policy set to OFF). To enable DTLS encryption, the system must be configured with a minimum security level of Best Effort.

Prevent GARP spoof attacks

On IP Phones that support it, Nortel recommends that you enable Gratuitous Address Resolution Protocol (GARP) Ignore, which protects against GARP Spoof attacks on the network. In a GARP Spoof attack, a malicious device on the network takes over an IP address (usually the default gateway) by sending unsolicited (or Gratuitous) ARP messages, thus manipulating the ARP table of the victim’s machine. This allows the malicious device to launch a variety of attacks on the network, resulting in undesired traffic routing. For more information about configuring IP Phones to protect the system from GARP spoof attacks, see *IP Phones Fundamentals* (NN43001-368).

> ***Note:*** To improve ARP security on clients that do not support GARP Ignore, you can investigate options such as configuring port security on the switch, implementing port-based authentication, or installing intrusion detection tools that monitor various network parameters and trigger alarm notifications if an attack pattern is detected. For more information about SIP Line, see *SIP Line Fundamentals* (NN43001-508).

Enable layer 2 authentication for IP Phones

Nortel recommends that you enable the 802.1x layer 2 device authentication feature. 802.1x authentication protects against unauthorized access by authenticating each IP Phone that is connected to the system. Supported 802.1x types are listed in Table 13 "Supported 802.1x types" (page 58). For more information about configuring 802.1x authentication, see *IP Phones Fundamentals* (NN43001-368).

Table 13
Supported 802.1x types

EAP-MD5
EAP-PEAP/MD5 (UNIStim 3 or later)
EAP-TLS (UNIStim 3 or later)

A Certificate Authority (CA) infrastructure is required for EAP-PEAP/MD5 and EAP-TLS.

Sign files

The system uses a Public Key Infrastructure (PKI) to validate certificates and other files downloaded to IP Phones. All firmware loads are signed by Nortel to protect the integrity of the files. If you use configuration files, Nortel recommends that you sign them so that they can be authenticated before installation on the phone. Authentication requires that the customer CA root certificate be installed on each phone. Once the customer CA root certificate is installed on the phone, all downloadable configuration files must be signed or they are rejected. For information about how to sign files and load certificates into IP Phones, see *IP Phones Fundamentals* (NN43001-368).

Security interactions

This section explains interoperability issues between security features and other system features or configurations.

Co-resident CP PM Call and Signaling Server

Communication Server 1000 Release 6.0 introduces the CP PM Co-resident Call and Signaling Server (CP PM Co-res CS and SS) which is capable of running the Call Server software, Signaling Server software, and System Management software on the same hardware platform operating under the RedHat Linux Operating System. For Communication Server 1000 Release 6.0, the only supported hardware platform for the CP PM Co-res CS and SS Server is the Call Processor-Pentium Mobile (CP PM) platform.

The key objective of co-residency is to provide a cost effective solution for Communication Server 1000 system installations that do not require high user capacity or the need for a redundant Call Server.

> ***Note:*** In Communication Server 1000 Release 6.0, the CP PM Co-res CS and SS does not support an HA configuration (dual core with Active/Inactive role). For systems that require HA configuration, the VxWorks-based Call Server software must be deployed.

Feature interactions within a Co-resident CP PM Call and Signaling Server use IP protocols for communication and work in the same manner as for standalone servers. However, Co-resident systems might affect the way in which some security features interact with various system components and applications.

For information about Co-resident CP PM Call and Signaling Server, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

ISSS and Element Manager on VxWorks signaling server

If you configure ISSS to Full Security, you must enable Secure Socket Layer/Transport Layer Security SSL/TLS for Element Manager, or Element Manager cannot operate on VxWorks signaling server. For an overview of the interaction of ISSS with Element Manager, see Table 14 "Interactions between ISSS and Element Manager web server on Signalling Server" (page 59).

Table 14
Interactions between ISSS and Element Manager web server on Signalling Server

ISSS configuration option	Access Element Manager through ELAN	Access Element Manager through TLAN
Full Security	Only using HTTPS[1]	[2]Using HTTPS or HTTP

Table 14
Interactions between ISSS and Element Manager web server on Signalling Server (cont'd.)

Functional Security, Optimized Security, No Security	Using either HTTP or HTTPS	[2]Using HTTPS or HTTP
[1]Note: The certificate for SSL must be installed on the signaling server"; for more information about certificate management see "Certificate creation and management" (page 103) [2]HTTP and HTTPS traffic on the TLAN is blocked if the Management Access in ELAN only flag is set on the Signalling Server.		

For more information about configuring SSL/TLS on Element Manager, see *Element Manager System Reference — Administration* (NN43001-632).

ISSS and Element Manager on UCM

If you are using Element Manager on UCM to manage Communication Server 1000 systems, Nortel recommends that you enable ISSS to protect confidentiality of communication between Element Manager and the Communication Server 1000 systems. ISSS is required to protect communication between Element Manager on UCM and the Communication Server 1000 systems because Xmsg protocol is used by Element Manager on UCM to communicate with Communication Server 1000 systems, and Xmsg provides neither encryption nor authentication. You must add the UCM IP addresses as external IPsec targets on the Communication Server 1000 system Call Server, and configure ISSS/IPsec for the Communication Server 1000 system on UCM; for more information see "IPsec configuration" (page 74).

UCM supports a unique ISSS/IPsec preshared key (PSK) for each Communication Server 1000 system managed by UCM. In the list of elements managed by UCM, you must enter the IPsec PSK for each managed Communication Server 1000 system, and it must be the same IPsec PSK that you use to configure ISSS on the Communication Server 1000 system Call Server. Nortel recommends that you change the IPsec PSK manually every few months. For more information about secret keys that you must refresh manually, see "Refresh system keys" (page 272).

ISSS and Geographic Redundancy

The Geographic Redundancy feature uses FTP to transfer customer configuration data from the Primary Call Server to the Secondary or Alternate Call Servers. You can protect FTP by configuring ISSS to use ISSS at the Full or Functional level. In either case you must configure the IPsec targets to protect FTP. Nortel recommends that you use ISSS between the primary and each secondary server; you must add the target for the primary to each secondary, and for each secondary to the primary.

The IPsec target list is unique to the individual Call Server, so you must configure the target on each server:

- Add each Secondary and Alternate Call Server to the IPsec target list on the Primary Call Server.
- Add the Primary Call Server to the IPsec target list on each Alternate Call Server.

For more information about the interaction of ISSS with FTP, see Table 15 "ISSS interaction with FTP" (page 61).

Table 15
ISSS interaction with FTP

ISSS configuration	IP target list	Result
FULL (Full)	not configured	FTP is blocked.
FULL (Full)	configured	FTP is permitted, and is protected by IPsec encryption.
FUNC (Functional)	not configured	FTP is permitted, but is not encrypted.
FUNC (Functional)	configured	FTP is permitted, and is protected by IPsec encryption.

ISSS/IPsec requires that all devices in the IPsec targets list, including the Primary, Secondary, and Alternate Call Servers, use the same preshared key (PSK) as the Unified Communications Management primary security server.

ISSS and AML

If you configure ISSS to Full Security, Applications Module Link (AML) connections to Symposium Call Center are still allowed but are not protected unless you define them as IPsec targets. The AML link to the Signaling Server of SIP CTI is protected by IPsec. If an auxiliary system is an ISSS manual target and configured with ISSS disabled, IPsec is not used; however, communication is restricted to identified manual targets.

IPsec is supported on CallPilot only with an Optimized or Functional security level.

ISSS and Port Access Restrictions and Linux firewall

When defining port access restrictions rules or configuring port-blocking using the Linux firewall (MFC), do not define rules that block critical system protocols on the ELAN. Although the port access restrictions feature has no effect on traffic received from targets protected by IPsec, these rules may come into effect when IPsec levels are changed and cause outages. Port blocking rules configured for the Linux firewall can impact traffic received from hosts protected by IPsec. Packets received from hosts that have enabled IPsec do not require firewall rules to be applied as these are trusted hosts.

ISSS and other protocols

If you configure ISSS to Full Security, connections using the following protocols are still allowed outside of the ISSS connection: SSH, SSL, and Network Time Protocol. Network Time Protocol has optional authentication and SSL and SSH are secure protocols, so ISSS is not required to protect them. AML traffic is not encrypted within known IPsec targets.

For information about adding an IPsec target manually, see "Add a new manual IPsec target" (page 78).

Media Security and call forwarding

Two types of call forwarding are available, and interact differently with Media Security, as follows:

- If you enable Unconditional Call Forward (CWFD), the originating IP Phone must match Media Security capabilities with the IP Phone that ultimately receives the call. The Media Security capabilities of the IP Phone that forwards the call are inconsequential.
- If you enable Call Forward No Answer (CFWDNA), the originating IP Phone must match security capabilities both with the IP Phone that forwards the call, and with the IP Phone that ultimately receives the call. If the IP Phone that is configured to use CFWDNA fails to match Media Security capabilities with the originating IP Phone, the call is disconnected without being forwarded.

Media Security and SIP phones

Media Security support the IETF standard (MIKEY NULL and SDESC), and interoperates with third-party SIP phones that also conform to these standards

If you enable Media Security on a system where both IP Phones capable of Secure Real Time Protocol (SRTP) connections and third-party SIP phones are installed, some third-party phones can reject incoming calls from the IP Phones. This can also prevent SIP phones from participating in conference calls. If calls fail between IP Phones and third-party SIP phones on your system, Nortel recommends that you configure the IP Phones to have a Class of Service for Media Security of Never (MSNV).

SIP phones are not able to participate in calls over SIP trunks if the far end device is using secure DSPs. SRTP capable DSPs (which are available on MGC and MC32S cards) are considered Best Effort secure by default. In such scenarios , it is recommended that Media Security be turned off in LD17 for all CS1000 systems.

Media Security Always and CallPilot mailboxes on systems without MGC daughterboards or MC32S

CallPilot traffic is not protected by Media Security on systems without MGC daughterboards or 32-channel Secure Media cards (MC32S). On these systems, IP Phones that are configured to use a Media Security Class of Service of Always cannot access CallPilot. For more information about the interaction of Media Security Class of Service with CallPilot access, see Table 16 "Interactions between Media Security and CallPilot on systems without MGC daughterboards or MC32S" (page 63).

Table 16
Interactions between Media Security and CallPilot on systems without MGC daughterboards or MC32S

Media Security Class of Service	Consequence
Media Security Always (MSAW)	Cannot access CallPilot.
Media Security Best Effort (MSBT) or Media Security Never (MSNV)	Can access CallPilot.

If you must configure Media Security with a Class of Service of MSAW, Nortel recommends that you install CallPilot in Media Gateway Controller (MGC) cabinets.

SIP TLS security policy interaction with Failsafe NRS

The SIP TLS Secure End-to-End and Secure Local policy settings prevent the operation of Failsafe NRS. If you are configuring TLS on a system where you use, or plan to use, Failsafe NRS, Nortel recommends that you use Best Effort policy for TLS. See Table 17 "Consequences of SIP trunk security" (page 63) for an explanation of the consequences of SIP TLS security configuration on Failsafe NRS.

Table 17
Consequences of SIP trunk security

SIP trunk security method	Consequence
TLS using Secure End-to-End or Secure Local policy	Failsafe NRS is not supported. SIP trunks are secured using TLS.

Table 17
Consequences of SIP trunk security (cont'd.)

TLS using Best Effort policy	Failsafe NRS is supported. SIP trunks are secured using TLS unless Failsafe NRS is in operation. Only trunks capable of SIP TLS are protected by TLS.
NonTLS SIP trunk security, such as a VPN gateway	Failsafe NRS is supported. SIP trunks are not secured using TLS.

SIP TLS interaction with SMC 2450

If a firewall such as the SMC 2450 Release 1.0 is installed with the system, verify that the port that is configured for TLS is opened (the default port for TLS is 5061). If you close this port, the firewall can interact with SIP TLS to prevent SIP trunks from communicating with the Signaling Server or SIP Proxy.

Recommendations for upgrading to Communication Server 1000 Release 6.0 from a previous release

The following is a high-level overview of the process for upgrading a Communication Server 1000 Release 5.x system to Release 6.0, as it pertains to system security.

> ***Note:*** This procedure does not apply to Geographic Redundancy configurations.

Prerequisites

- Depending on the needs and requirements of your system, not all steps described in this section may be applicable. Before proceeding with these upgrades, consult the applicable planning and engineering and upgrade guides to ensure that you understand the hardware, software, and networking requirements for your system.
- This procedure assumes that the system being upgraded is part of an IP Telephony network and thus requires a UCM primary security server and the ability of devices to register to the UCM security domain for Central Authentication. Standalone TDM-only systems do not require registration to the UCM security domain and thus do not require a UCM primary security server.

ATTENTION
Before beginning any upgrade, you must first backup the data on all servers being upgraded using the established backup method applicable to each system. For information about recommended backup practices for your system, refer to the applicable upgrade NTP.

Procedure 1
Upgrading to Communication Server 1000 Release 6.0 from a previous release

Step	Action
1	Install the UCM primary security server or upgrade an existing ECM server to Communication Server 1000 Release 6.0.
2	Restore the backup data to the server.
3	Upgrade the NRS primary and backup servers to Communication Server 1000 Release 6.0..
4	On the UCM primary security server, migrate (or create) the user accounts to be used for Central Authentication.
5	Complete the following steps for each pre-Release 6.0 system:

- If active, disable ISSS on each system and its elements by using Element Manager or the device CLI.
- Perform an Equipment Data Dump (EDD) and obtain the backup data.
- Remove the existing Signaling Servers from service. ISP1100 Signaling Servers are not supported in Communication Server 1000 Release 6.0 and must be replaced. Existing CP PM or COTS-based Signaling Servers can be upgraded if they meet the hardware requirements for Communication Server Release 6.0. For information on Signaling Servers, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- Install and configure the new Signaling Servers. You must designate one Signaling Server as the Element Manager host as multiple instances of Element Manager are not supported in Communication Server 1000 Release 6.0. These register with the UCM security domain during Linux base configuration.
- Upgrade the pre-Release 6.0 Call Servers to Communication Server 1000 Release 6.0, including database restoration. These register with the UCM security domain during Linux base configuration.
- Upgrade the firmware on VGMCs using Element Manager. MGCs automatically update to Release 6.0 firmware using FTP.

- Register the Call Server, MGCs, and VGMCs to the UCM security domain. For information about registering to the UCM security domain, see "Add or remove elements from the UCM security domain" (page 249)
- On the Call Server, configure Port Access Restrictions as desired for the Call Server, MGCs, and VGMCs.
- Disable insecure transfers and insecure shells as desired.
- If desired, configure ISSS defaults, add any manual targets, enable ISSS for the Call Server and its elements, then synchronize and activate. (You can defer this step until the entire network is upgraded.) For information about configuring ISSS, see "IPsec configuration" (page 74)

6 Generate a new security token, which is then synchronized automatically to all members of the UCM security domain. For information about generating security tokens, see "Regenerate the Secure FTP Token" (page 272)

7 On each Linux member, change the passwords for local system accounts, such as oam, pdt, root, and so on, as appropriate.

--End--

Migrate existing CS 1000 Release 5.x user accounts to CS 1000 Release 6.0

This section describes the planning considerations and procedures for migrating existing Communication Server 1000 Release 5.x user accounts to a Communication Server 1000 Release 6.0 system.

Prerequisites

Before beginning this procedure, review the following recommendations and planning considerations.

- All Communication Server 1000 Release 6.0 IP telephony systems and networked IP telephony solutions must be deployed in an existing enterpise-level UCM security domain. Communication Server 1000 Release 6.0 TDM-only systems may be optionally deployed in an existing UCM domain or without UCM.
- When planning to upgrade Communication Server 1000 pre-Release 6.0 systems and networked IP telephony solutions, the Release 6.0 UCM security domain must already be established.
- All existing Communication Server 1000 OAM and PDT user accounts must be manually created in the Release 6.0 UCM primary security server before starting to upgrade any pre-Release 6.0 Communication Server 1000 systems and system elements.

- For Communication Server 1000 IP telephony solutions, some OAM and PDT user accounts must have role-based access with the appropriate permissions for a subset of all Communication Server 1000 systems in the UCM security domain.
- System-specific CS 1000 OAM/PDT roles must be manually mapped by the UCM AAA network administrator to each individual Communication Server 1000 system element.

  Note: Users assigned to a predefined system role gain access to all system elements associated with that role. Multiple users may require specific access and restrictions beyond the capabilities of the default user roles. In this event, you must configure custom roles for those users.While you can define user access to the CLI of individual system elements using an instance of Element Manager, the only way to grant CLI access to the Signaling Servers for users assigned to custom roles is on a one-by-one basis.

- All OAM/PDT user account passwords must be reset when migrating to Release 6.0 UCM security domain and Communication Server 1000 Release 6.0. Due to password reset, each OAM/PDT account user must first access the UCM primary server by entering the FQDN of the UCM primary or backup server, or the FQDN of any registered Linux/UCM base element, and changing the initial reset password.

Procedure 2
Migrating existing CS 1000 Release 5.x user accounts to CS 1000 Release 6.0

Step	Action
1	For each server in the system, complete the following: • Log on to the Call Server using a PWD2 user account with user account management permissions. • Using LD 17, print out all PWD2, PWD1, PDT2, PDT1, and limited access system administration accounts. • Capture the print out of accounts for each system in a text file. To facilitate the migration of a large number of accounts, you can import the text files containing the print out of user accounts for each system into a spreadsheet of your own design.
2	Determine which existing Communication Server 1000 user accounts OAM and problem determination roles are authorized to access all Communication Server 1000 systems in the enterprise-wide UCM domain.

These user accounts will migrate to UCM Authentication, Authorization, and Auditing (AAA) accounts that are mapped in the UCM primary server to the same roles on all Communication Server 1000 systems.

> ***Note:*** Access to the same roles on all UCM base elements in the UCM domain includes access to Linux/UCM base manager and Linux CLI of all UCM member elements, including all NRS instances, and UCM primary and backup servers.

3 Determine which existing Communication Server 1000 user accounts OAM and problem determination roles are authorized to access only a subset of Communication Server 1000 systems in the enterprise-wide UCM domain.

These user accounts will migrate to the UCM AAA accounts that are mapped in the UCM primary security server to specially configured roles that have access only to specified Communication Server 1000 Element Manager instances, and to specified Communication Server 1000 system elements.

--End--

ISSS

This chapter contains procedures to help you protect intrasystem signaling and signaling between the system and its management applications using Intrasystem Signaling Security (ISSS)/IP security (IPsec). The chapter is divided into the following sections:

- “ISSS overview” (page 69)
- “IPsec configuration” (page 74)
- “Other ISSS configuration and maintenance procedures” (page 87)

CAUTION

When a Communication Server 1000 5.5 or earlier system is upgraded to Release 6.0, the existing IPsec configurations are disabled and must be re-configured using the Unified Communications Management primary security server interface.

During the upgrade, intra-network communications between elements are interrupted and non-operational. Also, intra-network communication reverts to an insecure state after the upgrade is completed.

ISSS overview

IP security for Communication Server 1000 networks is centrally managed from the Unified Communications Management 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. This feature includes industry-standard encryption algorithms from the openSSL Crypto Library.

Communication Server 1000 provides simplified, automated IPsec policy configuration and avoids the complex configuration requirements inherent in many other implementations of IPsec.

ISSS elements are classified into the following two categories:

- UCM Targets—these elements automatically belong to the Unified Communications Management security domain without the need to add them using the Unified Communications Management ISSS management interface. An example of a Unified Communications Management target is a Call Server.
- Manual targets—these elements must be manually configured using the Unified Communications Management ISSS management interface before ISSS can be enabled. An example of a manual target is Call Pilot.

When a new device is installed and configured as part of the UCM security domain it is automatically listed in the UCM targets table. Devices that are not part of the UCM security domain must be added as Manual targets from the ISSS user interface.

ISSS can manage up to a maximum of 1500 combined Unified Communications Management and manual targets.

ISSS/IPsec only secures IP traffic on the ELAN. At Full security level, the AML protocol is protected on the TLAN of Linux-based elements for manual targets. You can protect any feature within the ELAN depending on the Security Level, as described in Table 18 "ISSS/IPsec security levels" (page 70).

Table 18
ISSS/IPsec security levels

ISSS/IPsec security level	Description
Optimal	(OPTI) ELAN traffic over pbxLink and Xmsg between this host and its known IPsec targets is protected by IPsec. IPsec is required for both pbxLink and Xmsg. For unknown IPsec targets, traffic using the pbxLink and Xmsg protocols is denied.
Full	(FULL) For known IPsec targets, all ELAN protocols except HTTPS, LDAPS, RADIUS, BOOTP, SSH/sFTP, SSL/TLS, and DTLS are protected by IPsec. For unknown IPsec targets, all protocols are denied IPsec, except HTTPS, LDAPS, RADIUS, BOOTP, SSH/sFTP, SSL/TLS, and DTLS. If Full security is configured on the CS 1000 system, all external devices such as CallPilot and TM must have IPsec configured in order to communicate with the CS 1000 system. These auxiliary devices can communicate without IPsec if they are configured as ISSS Disabled in UCM.

Table 19 "Security levels and port protection for IPsec" (page 71) shows ISSS security levels and how they relate to protected ports for IPsec:

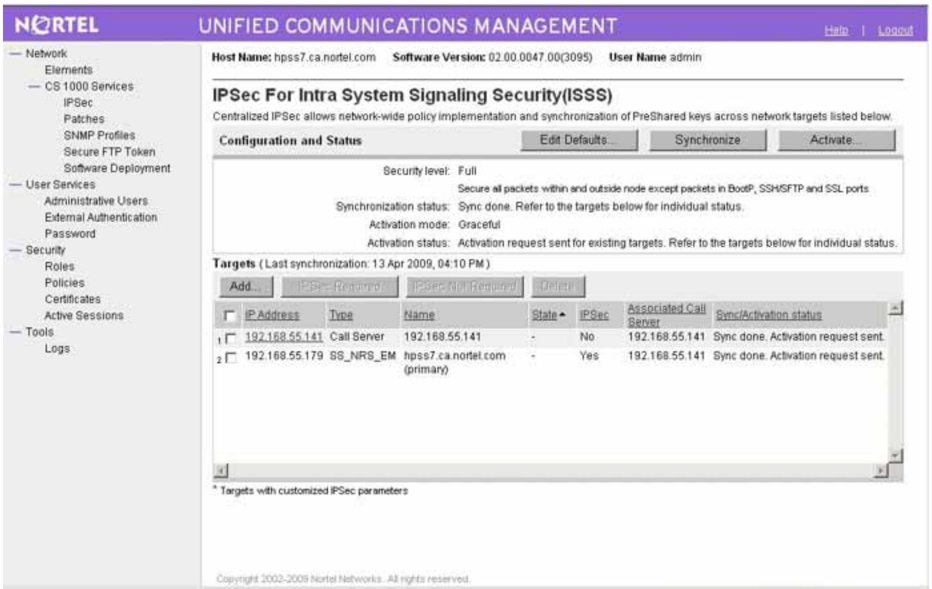
Table 19
Security levels and port protection for IPsec

ISSS Level	IPsec protected ports	
Optimal	**Known targets**	**Unknown targets**
	The following ports are protected with IPsec: • 15000 (TCP/UDP) • 15001 (UDP) • 15080 (TCP) • 15081 (TCP)	Unknown targets are denied on the following ports: • 15000 (TCP/UDP) • 15001 (UDP) • 15080 (TCP) • 15081 (TCP)
Full	**Known targets**	**Unknown targets**
	Protected ports: • All Exceptions (permitted without IPsec): • 22 (TCP) • 67(UDP) • 68(UDP) • 443(TCP) • 636 (TCP) • 1812 (UDP)	Protected ports • All Exceptions (permitted without IPsec): • 22 (TCP) • 67(UDP) • 68(UDP) • 443(TCP) • 636 (TCP) • 1812 (UDP)

Unified Communications Management IPsec ISSS management interface page

The IPsec management and configuration page is located at **Network > CS-1000 Services > IPsec**. When you navigate to this link from the Unified Communications Management main navigation menu, the IPsec for Intra System Signaling Security page appears, as shown in Figure 2 "IPsec for Intra System Signaling Security page in UCM" (page 72).

Figure 2
IPsec for Intra System Signaling Security page in UCM



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0047.00(3095) **User Name** admin

IPSec For Intra System Signaling Security(ISSS)

Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.

Configuration and Status

Security level:	Full Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports
Synchronization status:	Sync done. Refer to the targets below for individual status.
Activation mode:	Graceful
Activation status:	Activation request sent for existing targets. Refer to the targets below for individual status.

Targets (Last synchronization: 13 Apr 2009, 04:10 PM)

	☐	IP Address	Type	Name	State ▲	IPSec	Associated Call Server	Sync/Activation status
1	☐	192.168.55.141	Call Server	192.168.55.141	-	No	192.168.55.141	Sync done. Activation request sent.
2	☐	192.168.55.179	SS_NRS_EM	hpss7.ca.nortel.com (primary)	-	Yes	192.168.55.141	Sync done. Activation request sent.

* Targets with customized IPSec parameters

Copyright 2002-2009 Nortel Networks. All rights reserved.

From the ISSS interface on the Unified Communications Management primary security server, you can administer several aspects of IP security, such as the configuration of a domain-wide security policy, the adding and removing of IPsec targets, and the enabling or disabling of IPsec for network elements.

WARNING
If you configure a network element as Enabled, it must communicate using IPsec as defined by the current level (OPTI or FULL). If you configure the element as Disabled, it continues to communicate with the other elements without IPsec protection. This is not recommended as it may create a security vulnerability. Do not run the scanner on the ELAN directly.

Elements that are managed by ISSS require a centrally-configured password or preshared key (PSK) to allow for the detection of devices that do not have the correct credentials and to prevent unauthorized access.

The ISSS configuration page contains two main sections, the Configuration and Status area and the Targets table. The Configuration and Status area displays the current security level, synchronization status, and activation status for all targets. You can edit, synchronize, and activate these configurations by clicking the Edit Defaults, Synchronize, or Activate buttons.

The Targets table lists all targets for which the current IPsec configurations are applicable. By default, all applicable Unified Communications Management elements appear in this table and are sorted by State. You can modify targets by clicking the Add, IPSec Required, IPSec Not Required, or Delete buttons.

Table 20 "IPsec Targets table item descriptions" (page 73) shows the Target table items and a description of the information each column contains.

Table 20
IPsec Targets table item descriptions

Item	Description
IP Address	ELAN IP of the IPsec target.
Type	Type of the IPsec target.
Name	Friendly name of the IPsec target.
State	Displays the state of the target, where: • NEW—the target has not been synchronized • DELETED—the target had been synchronized, but was deleted • "_"—the target has previously been synchronized
IPsec	Displays whether IPsec is required or not required for a target. This represents the locally saved status for the target; changes to the IPsec status of targets do not appear until the synchronization and activation process has been completed.
Associated Call Server	Displays the Associated Call Server for the element. If there is no Associated Call Server, this field is blank.
Sync/Activation status	Displays the last synchronization status. If no status is available, this field is blank.

The Synchronization status displays a message indicating the current status. The following list describes the Synchronization and Activation status messages and their meanings:

- **Synchronizing.** This message displays if synchronization is in progress.
- **Sync done. Activation required.** This message displays after synchronization completes but activation has not yet taken place.
- **Sync done. Activation request sent.** This message displays after synchronization and activation completes.
- **Sync done. Activation request failed.** This message displays after synchronization completes but activation has failed.

- **Sync done. Sending activation request...** This message displays after synchronization completes and activation is in progress.
- **Sync failed.** This message displays if synchronization fails due to system or network problems.

> **ATTENTION**
> The following restrictions apply to ISSS/IPsec:
>
> - To use ISSS, you must upgrade all components to Communication Server 1000 Release 6.0.
> - On VxWorks-based devices, IPsec applies only to the ELAN.

ISSS synchronization and activation

When configuring ISSS parameters, two steps are required to put the new configurations into effect. The synchronization phase, which delivers the new parameters to the UCM members, and the activation phase, which instructs the UCM members to place the new parameters into effect.

There are two activation modes, Graceful and Forced. Graceful activation results in a seamless activation of the new parameters to unaffected targets in most situations; however, changes to the PSK do not take effect until existing sessions expire, which in some cases can take up to three days.

Forced activation causes immediate use of a newly configured PSK; however, messaging traffic is disrupted, causing a service interruption that can last for several minutes. Nortel recommends that you only use Forced activation during scheduled maintenance periods.

IPsec configuration

Use the procedures in this section to configure IPsec using the interface of the Unified Communications Management primary security server.

Prerequisites

- ISSS configuration on Unified Communications Management is restricted to those who have Administrator access to the primary security server.

Configure ISSS for a new installation

After a new (or "fresh") installation, when the IPsec for Intra System Signaling Security (ISSS) page is loaded for the first time the security level is undefined. All devices that are part of the UCM security domain are listed in the Targets table.

To configure ISSS after a new installation, complete the following steps.

Procedure 3
Configuring ISSS for a new installation

Step **Action**

1 Log in to the UCM primary security server and navigate to **CS 1000 Servers > IPSec**.

The IPSec for Intra System Signaling Security (ISSS) page displays.

2 (Optional) If applicable, add and configure any manual targets. Manual targets are targets that are not registered to the UCM security domain. If no manual targets are required, you can skip this step.

For the procedure to add a manual target, see “Add a new manual IPsec target” (page 78).

3 (Optional) Disable IPsec for any desired targets. If IPsec is required for all targets, you can skip this step.

Under normal operating conditions, you would not disable IPsec; however, under certain conditions, you may wish to disable IPsec for a target. Some reasons for not configuring IPsec on a target include:

- The target is not configured for IPsec or is not capable of communications using IPsec.
- New or replacement elements, such as MGCs and Media Cards that require a firmware upgrade before being able to register with UCM, may need to have IPsec disabled until they are able to re-register with the UCM security domain and obtain the ISSS configurations.

For the procedure to disable IPsec for targets, see “Enable or disable IPsec for a target” (page 80).

4 Configure the default IPsec settings. For the procedure to configure the default IPsec settings, see “Configure default IPsec settings” (page 76).

5 (Optional) Configure customized IPsec settings for a Call Server and its elements. If customized settings are not needed, you can skip this step.

For the procedure to configure customized settings, see “Customize IPsec for a Call Server target” (page 82).

6 Activate the IPsec configuration.

For the procedure to activate the IPsec configuration, see "Activate IPsec configuration settings" (page 84).

--End--

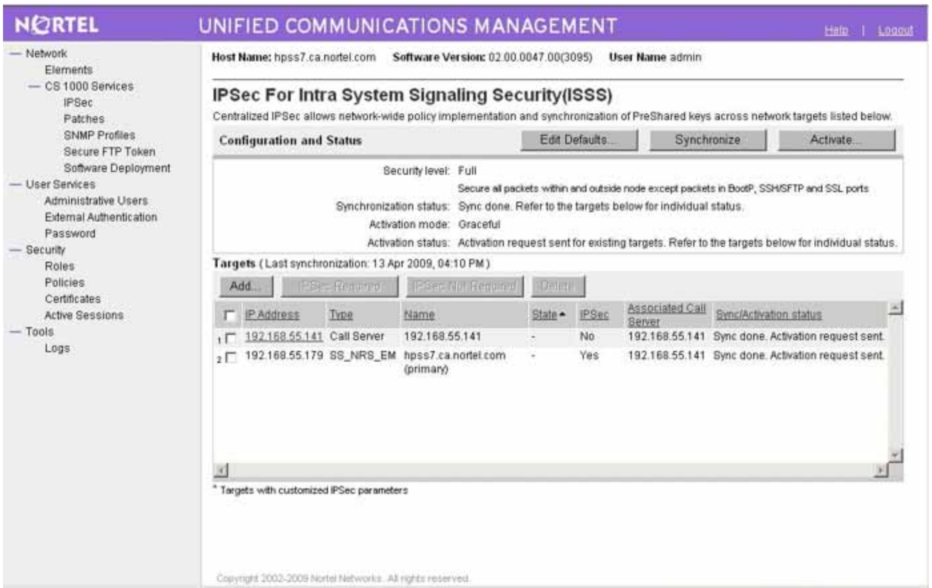
Configure default IPsec settings

Use this procedure to configure the default IPsec settings.

> **ATTENTION**
> During the activation of ISSS parameters, there may be temporary disruption to internal system messaging. As a result, various system events may be reported and service may be impacted. The system recovers from these interruptions once activation is complete on all communicating members. The impact of activation depends on the type of change and the options selected, as indicated below.
>
> When modifying ISSS levels on a Communication Server 1000 system or activating changes in forced mode, you should schedule the activation during a maintenance window for all affected call servers. In the worst case scenario, disruptions may last for several minutes, with the duration generally increasing with the number of members in the UCM security domain. Typical disruptions should be less than 1 minute.
>
> The activation of changes within a specific ISSS level that are requested with graceful activation, including the addition or removal of targets, enabling or disabling of ISSS for targets, and changes to the PSK, have minimal impact on system operations and are isolated to the new or modified targets. This is the normal mode of operation once the ISSS level has been configured for a Communication Server 1000 system.

Procedure 4
Configuring default IPsec settings

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**. The IPSec For Intra System Signaling Security (ISSS) page displays.



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0047.00(3095) **User Name** admin

IPSec For Intra System Signaling Security(ISSS)

Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.

Configuration and Status

Security level: Full
Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports
Synchronization status: Sync done. Refer to the targets below for individual status.
Activation mode: Graceful
Activation status: Activation request sent for existing targets. Refer to the targets below for individual status.

Targets (Last synchronization: 13 Apr 2009, 04:10 PM)

	□	IP Address	Type	Name	State ▴	IPSec	Associated Call Server	Sync/Activation status
1	□	192.168.55.141	Call Server	192.168.55.141	-	No	192.168.55.141	Sync done. Activation request sent.
2	□	192.168.55.179	SS_NRS_EM	hpss7.ca.nortel.com (primary)	-	Yes	192.168.55.141	Sync done. Activation request sent.

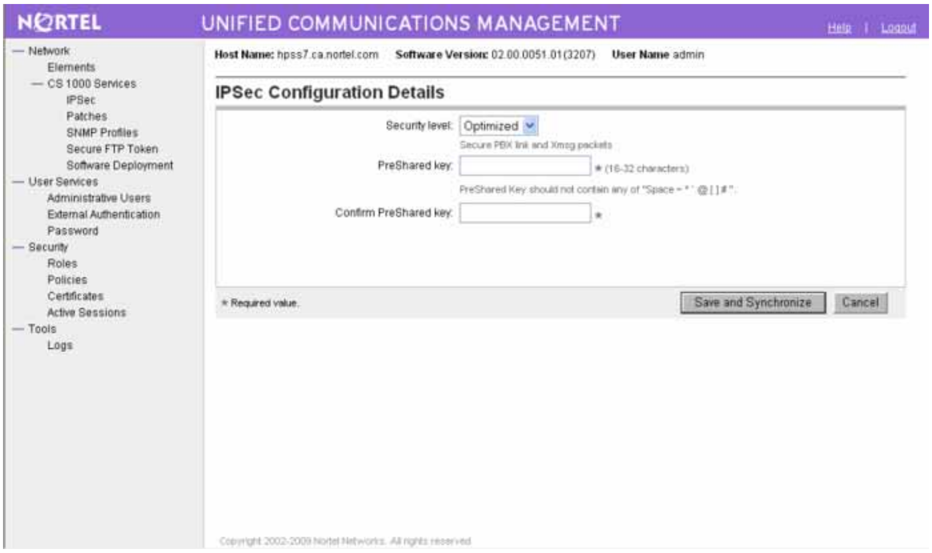
* Targets with customized IPSec parameters

Copyright 2002-2009 Nortel Networks. All rights reserved.

3 In the Configuration and Status section, click **Edit Defaults**.

The IPsec Configuration Details page displays, as shown in Figure 3 "IPsec Configuration Details page" (page 77).

Figure 3
IPsec Configuration Details page



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0051.01(3207) **User Name** admin

IPSec Configuration Details

Security level: Optimized
Secure PBX link and Xmsg packets
PreShared key: * (16-32 characters)
PreShared Key should not contain any of "Space = " ' @ [ ] # ".
Confirm PreShared key: *

* Required value.

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 Select the desired Security Level and enter the appropriate PreShared key. You must enter the PreShared key again to confirm.

Note 1: All geographically redundant Call Servers must be configured with same Security Level and pre-shared key as the Primary Call Server.

> ***Note 2:*** For new installs there is no pre-shared key so you must supply one. For upgrades, the pre-shared key is preserved but not displayed on the screen (the characters are masked, as with passwords).

5 Click **Save and Synchronize** to save and synchronize the changes.

The default settings are applied to all elements associated with the Call Server.

6 Click **Cancel** to return to the IPsec details page.

--End--

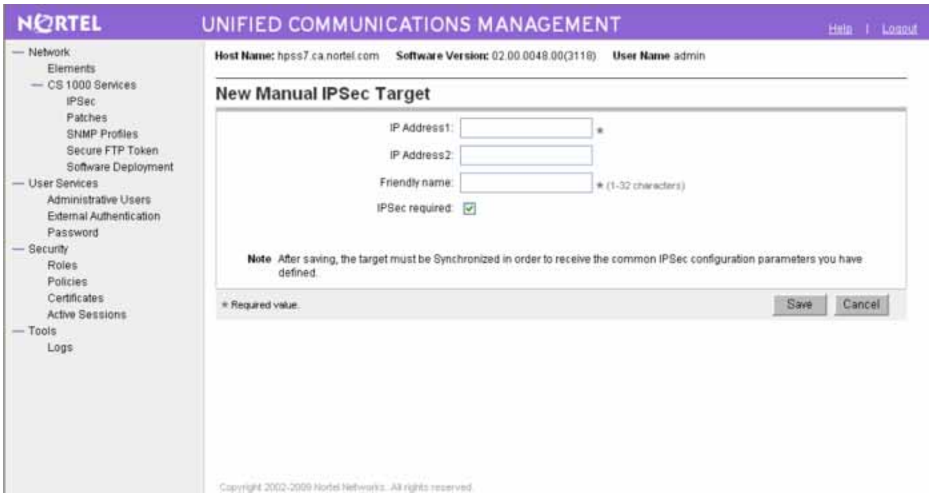
Add a new manual IPsec target

Use this procedure to add a new manual IPsec target. Manual targets are targets that are not registered to the UCM security domain.

Procedure 5
Adding a new manual IPsec target

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**.
3	Click **Add**. The New Manual IPsec Target page displays, as shown in Figure 4 "New Manual IPsec Target page" (page 78).

Figure 4
New Manual IPsec Target page



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0048.00(3118) **User Name** admin

New Manual IPSec Target

IP Address1: *
IP Address2:
Friendly name: * (1-32 characters)
IPSec required: ☑

Note After saving, the target must be Synchronized in order to receive the common IPSec configuration parameters you have defined.

* Required value.

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 Obtain the following information and enter it into the appropriate fields:

- IP address 1—the IP address of the target

  Note: If a manual target IP matches either the ELAN/TLAN IP of an automatically discovered UCM target, then the manual target is replaced by the automatically discovered UCM target. This avoids duplicate entries in IPsec configurations.

- IP address 2—the second network interface of the manual target, if available
- Friendly name—a user-chosen name for the target (1 to 32 characters)

5 Ensure the **Enable IP Security** check box is selected.

Note: Deselecting the IPSec required check box allows the target to communicate with other elements in the system that are configured at FULL level using IP address 1.

6 Click **Save**.

You are returned to the main IPsec page, which displays the appropriate synchronization status.

7 Click **Cancel**.

Note: The new manual IPsec target will communicate with all other IPsec targets. However, the IPsec settings are not transferred to the manual targets as there is no provision to associate manual targets to particular elements they can communicate with.

--End--

Edit an existing manual IPsec target

Use this procedure to edit the configuration settings for an existing IPsec manual target.

Procedure 6
Editing an existing manual IPsec target

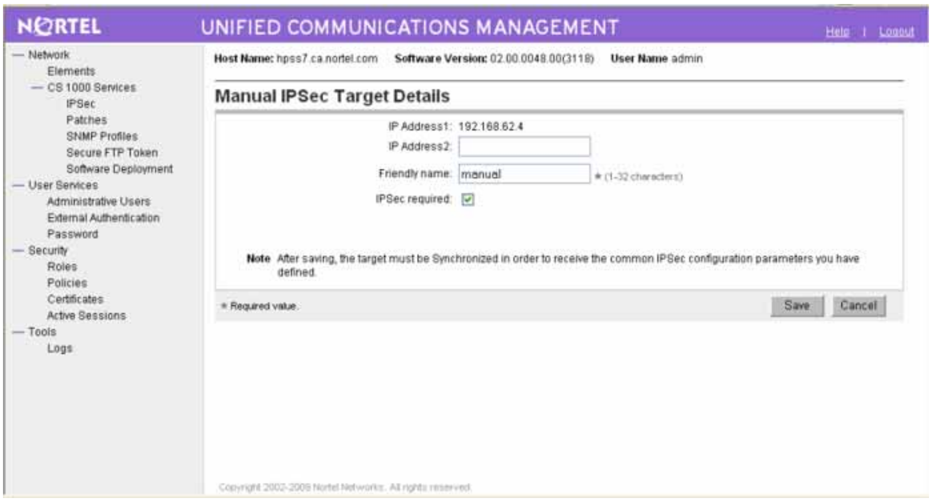
Step	Action
1	Log on to the UCM primary security server.

2 From the navigation tree, select **Network > CS 1000 Services > IPsec**.

3 From the Targets table, select a manual target IP Address link.

The Manual IPsec Target Details page appears, as shown in Figure 5 "Manual IPsec Target Details" (page 80).

Figure 5
Manual IPsec Target Details



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0048.00(3118) **User Name** admin

Manual IPSec Target Details

IP Address1: 192.168.62.4

IP Address2:

Friendly name: manual * (1-32 characters)

IPSec required: ☑

Note After saving, the target must be Synchronized in order to receive the common IPSec configuration parameters you have defined.

* Required value.

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 Make the desired changes to the configuration settings.

5 Click **Save**.

6 Click **Cancel** to return to the IPsec details page.

--End--

Enable or disable IPsec for a target

Use this procedure to enable or disable IPsec for a target.

Procedure 7
Enabling or disabling IPsec for a target

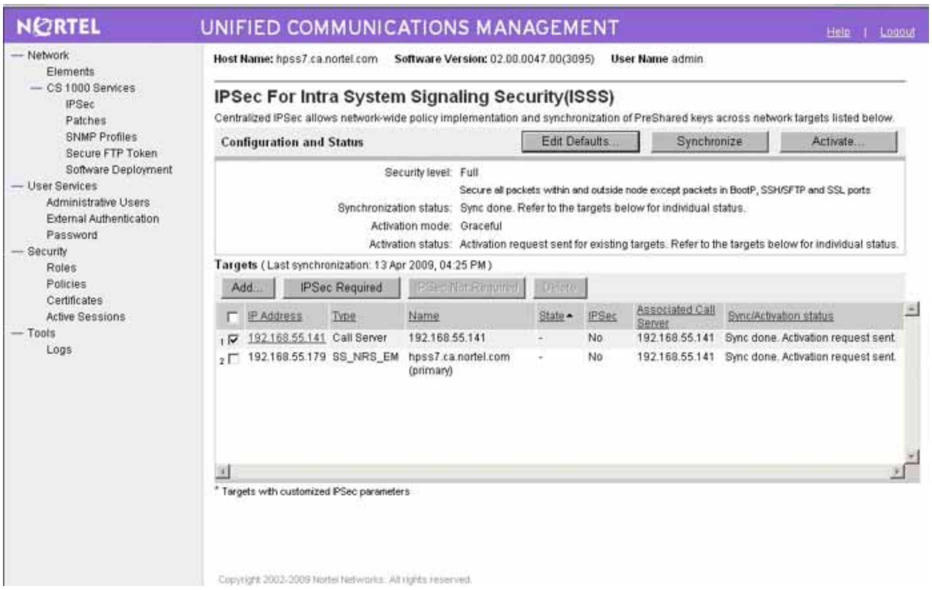
Step	Action

1 Log on to the UCM primary security server.

2 From the navigation tree, select **Network > CS 1000 Services > IPsec**.

The **IPsec For Intra System Signaling Security (ISSS)** page displays, as shown in Figure 6 "IPsec For Intra System Signaling Security (ISSS) page" (page 81).

Figure 6
IPsec For Intra System Signaling Security (ISSS) page



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0047.00(3095) **User Name** admin

IPSec For Intra System Signaling Security(ISSS)

Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.

Configuration and Status

Security level: Full
Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports
Synchronization status: Sync done. Refer to the targets below for individual status.
Activation mode: Graceful
Activation status: Activation request sent for existing targets. Refer to the targets below for individual status.

Targets (Last synchronization: 13 Apr 2009, 04:25 PM)

	□	IP Address	Type	Name	State ▲	IPSec	Associated Call Server	Sync/Activation status
1	☑	192.168.55.141	Call Server	192.168.55.141	-	No	192.168.55.141	Sync done. Activation request sent.
2	□	192.168.55.179	SS_NRS_EM	hpss7.ca.nortel.com (primary)	-	No	192.168.55.141	Sync done. Activation request sent.

* Targets with customized IPSec parameters

Copyright 2002-2009 Nortel Networks. All rights reserved.

3 From the Targets table, select the check box for each target to be enabled or disabled.

4 Do one of the following:

To enable the selected targets, click **IPsec Required**.

OR

To disable the selected targets, click **IPsec Not Required**.

IPsec for all of the selected targets is enabled or disabled.

If you've made changes, the following message displays in the Configuration and Status section: “Configuration changed. Sync required." Otherwise, the current status displays.

> ***Note:*** After configuring IPsec as Yes or No for selected targets, you must initiate the synchronization process.

5 Click **Synchronize**.

--End--

Delete a manual target

Use this procedure to delete a manual target.

Procedure 8
Deleting a manual target

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**.
3	From the Targets table, select the check box for each manual target to be deleted.
4	Click **Delete**. The selected targets are deleted and the following message displays: “New or Deleted Targets found. Sync required.” ***Note:*** After deleting selected targets, you must initiate the synchronization process.
5	From the main IPsec page, click **Synchronize**.
6	Click the IPsec link to get the latest synchronization status. ***Note:*** If a new target is deleted, this target is directly removed from targets table and the deleted status is not shown for it.

--End--

Customize IPsec for a Call Server target

Use this procedure to customize the IPsec settings for a Call Server target. By default, all targets use the default IPsec settings. However, you can customize a Call Server to have its own IPsec settings.

Customization ensures that the Call Server and all of its associated elements use the same ISSS Level and PSK, but ones that are different from the default ISSS Level and PSK.

You cannot define a customized configuration without first defining the default configuration.

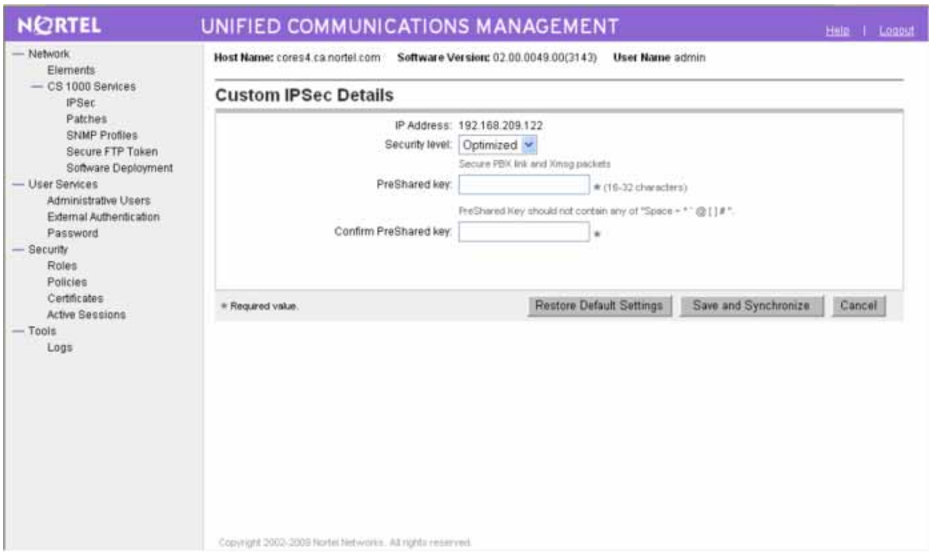
Procedure 9
Customizing IPsec for a Call Server target

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**.

3 From the Targets table, select the IP address of the CS 1000 Call Server target you want to customize.

The Custom IPsec Details page displays, as shown in Figure 7 "Custom IPsec Details page" (page 83).

Figure 7
Custom IPsec Details page



Host Name: cores4.ca.nortel.com **Software Version:** 02.00.0049.00(3143) **User Name** admin

Custom IPSec Details

IP Address: 192.168.209.122

Security level: Optimized

Secure PBX link and Xmsg packets

PreShared key: * (16-32 characters)

PreShared Key should not contain any of "Space = * ' @ [ ] # ".

Confirm PreShared key: *

* Required value.

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 From the Security level list, select the desired level of security.

5 Enter the appropriate Pre-shared key. You must enter the Pre-shared key again to confirm.

> ***Note:*** All Call Servers in a Geographic Redundancy configuration must be configured with same Security Level and Pre-shared key as the Primary Call Server.

6 Click **Save and Synchronize** to save and synchronize the changes.

After synchronization completes, the customized settings are transferred to all targets within the security domain, not just the customized Call Server and its associated elements.

Customized elements appear in the Targets table marked with an asterisk (*).

> ***Note:*** After synchronization completes, activation is required for the new configuration changes to take effect.

You can perform this procedure for all Call Servers requiring customized IPsec configurations.

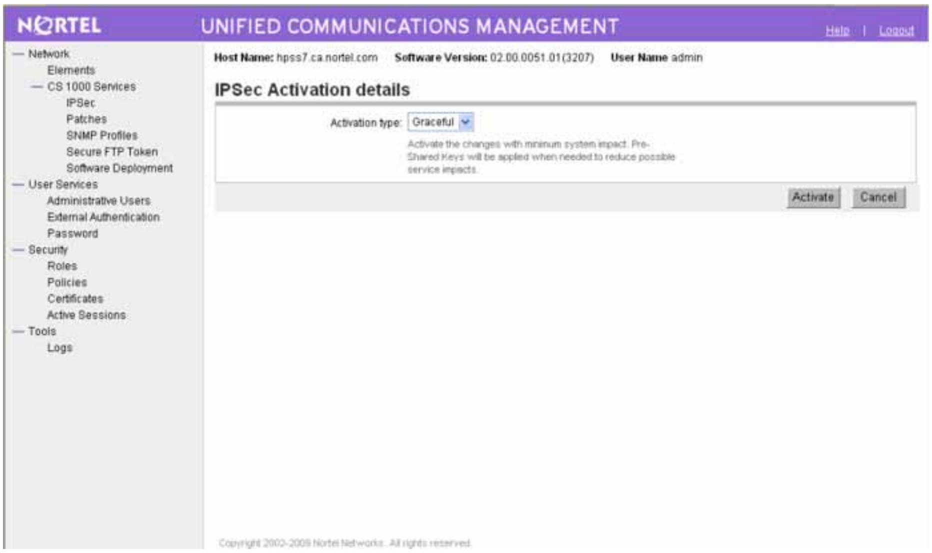
--End--

Activate IPsec configuration settings

Use this procedure to activate the IPsec configuration settings. You must activate for the configuration settings to take effect. Activation sends the activate request to all the targets in the security domain. On receiving the activation request, all the targets activate the IPsec configurations already defined and synchronized.

Procedure 10
Activating the IPsec configuration settings

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**.
3	Click **Activate**. The IPsec Activation details page appears.



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0051.01(3207) **User Name** admin

IPSec Activation details

Activation type: Graceful

Activate the changes with minimum system impact. Pre-Shared Keys will be applied when needed to reduce possible service impacts.

Copyright 2002-2009 Nortel Networks. All rights reserved.

Step	Action
4	From the **Activation type** menu, select the activation mode. You can choose Graceful or Forced. If you select Graceful activation, the following message appears:

Activate the changes with minimum system impact. Pre-Shared Keys will be applied when needed to reduce possible service impacts.

If you select Forced activation, the following message appears:

Activate the changes and force immediate use of all new settings. Services will be temporarily interrupted.

5 Click **Activate**.

6 Click **Cancel** to return to the IPsec details page.

--End--

Synchronize IPsec configuration settings

Use this procedure to synchronize the IPsec configuration changes. You only need to synchronize manually if you have enabled or disabled IPsec for a target, or if you have deleted a manual target.

Procedure 11
Synchronizing IPsec configuration settings

Step	Action

1 Log on to the UCM primary security server.

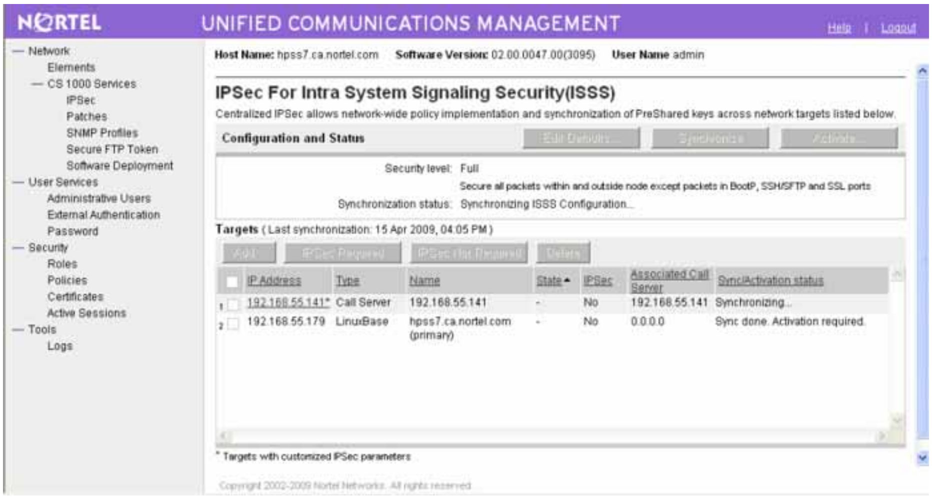
2 From the navigation tree, select **Network > CS 1000 Services > IPsec**.

3 Click **Synchronize**.

The synchronization process initiates. The **Synchronize** button is dimmed (disabled).

4 From the navigation tree, click **IPsec** to retrieve the latest synchronization status.

In the Configuration and Status section, under Synchronization status, the following message displays: "Sync done. Refer to the targets table below for individual status".



Host Name: hpss7.ca.nortel.com **Software Version:** 02.00.0047.00(3095) **User Name** admin

IPSec For Intra System Signaling Security(ISSS)

Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.

Configuration and Status

Security level: Full
Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports
Synchronization status: Synchronizing ISSS Configuration...

Targets (Last synchronization: 15 Apr 2009, 04:05 PM)

		IP Address	Type	Name	State ▲	IPSec	Associated Call Server	Sync/Activation status
1	□	192.168.55.141*	Call Server	192.168.55.141	-	No	192.168.55.141	Synchronizing...
2	□	192.168.55.179	LinuxBase	hpss7.ca.nortel.com (primary)	-	No	0.0.0.0	Sync done. Activation required.

* Targets with customized IPSec parameters

Copyright 2002-2009 Nortel Networks. All rights reserved.

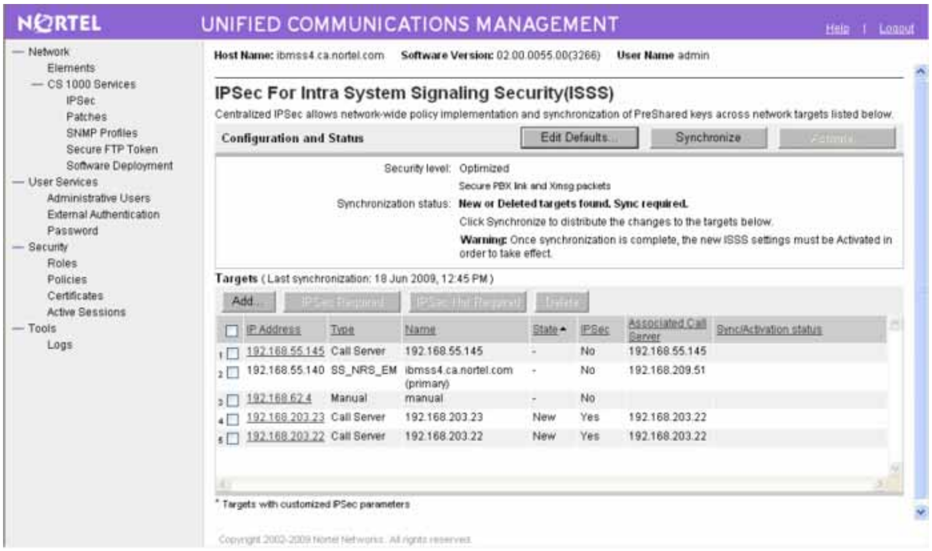
--End--

Configure ISSS when a new element joins the security domain

When a new element joins the security domain, you must perform a synchronization and activation. When a new element, such as a MGC or media card, is added to the security domain, perform the activation of the updated ISSS parameters in Graceful mode to minimize any potential system interruptions.

When activating ISSS in Graceful mode, only the IP traffic of the updated elements is impacted. All existing security associations are maintained and only the rules for the updated members are deleted or added on each of the other elements.

Step	Action
1	Log on to the UCM primary security server.
2	From the navigation tree, select **Network > CS 1000 Services > IPsec**. The **IPsec For Intra System Signaling Security (ISSS)** page displays. In the Targets table, new elements are shown with New in their State column.



Host Name: ibmss4.ca.nortel.com **Software Version:** 02.00.0055.00(3266) **User Name** admin

IPSec For Intra System Signaling Security(ISSS)

Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.

Configuration and Status

Security level: Optimized

Secure PBX link and Xmsg packets

Synchronization status: **New or Deleted targets found. Sync required.**

Click Synchronize to distribute the changes to the targets below.

Warning: Once synchronization is complete, the new ISSS settings must be Activated in order to take effect.

Targets (Last synchronization: 18 Jun 2009, 12:45 PM)

	□	IP Address	Type	Name	State ▲	IPSec	Associated Call Server	Sync/Activation status
1	□	192.168.55.145	Call Server	192.168.55.145	-	No	192.168.55.145	
2	□	192.168.55.140	SS_NRS_EM	ibmss4.ca.nortel.com (primary)	-	No	192.168.209.51	
3	□	192.168.62.4	Manual	manual	-	No		
4	□	192.168.203.23	Call Server	192.168.203.23	New	Yes	192.168.203.22	
5	□	192.168.203.22	Call Server	192.168.203.22	New	Yes	192.168.203.22	

* Targets with customized IPSec parameters

Copyright 2002-2009 Nortel Networks. All rights reserved.

3 In the Configuration and Status area, click **Synchronize**.

After the synchronization completes, the status is displayed as "Activation required".

4 Click **Activate**.

5 From the **Activation type** menu, select Graceful activation mode.

> ***Note:*** When a new element, such as a MGC or media card, is added to the security domain, perform the activation of the updated ISSS parameters in Graceful mode to minimize any potential system interruptions. When activating ISSS in Graceful mode, only the IP traffic of the updated elements is impacted. All existing security associations are maintained and only the rules for the updated members are deleted or added on each of the other elements.

6 Click **Activate**.

The IPsec configurations are transferred to the targets.

--End--

Other ISSS configuration and maintenance procedures

This section contains ISSS/IPsec maintenance and configuration procedures.

Maintenance on Linux servers

Use the procedures in this section to perform maintenance of ISSS/IPsec on Linux hosts.

Change ISSS/IPsec PSK on UCM Linux host with NRS Manager using CLI

Nortel recommends that you change the IPsec PSK periodically to improve the security in your system.

Use the following procedure to replace an existing IPsec target.

Procedure 12
Changing the ISSS/IPsec PSK on UCM Linux host

Step	Action
1	Log on to the Command Line Interface (CLI) of the Linux server using the account nortel.
2	Enter: `deleteIPsectarget <IP address>` A prompt appears requesting that you enter the root password.
3	Enter the root password.
4	Enter `newIPsectarget <IP address> <IPsec PSK> <ISSS level>`. A prompt appears requesting that you enter the root password.
5	Enter the root password.

--End--

Table 21
Variable definitions

Variable	Value
<IP address>	The IP address of the IPsec target to be deleted or created.
<IPsec PSK>	The IPsec PSK to assign to the element.
<ISSS level>	The IPsec security level to assign to the element.

Use the following procedure to view configuration information for each IPsec target configured on a Linux server.

Procedure 13
Viewing IPsec target configurations for UCM certificate manager coresident with an NRS Manager

Step	Action
1	Log on to the CLI of the Linux server using the account nortel.

2 Enter:
`checkIPsecStatus .`

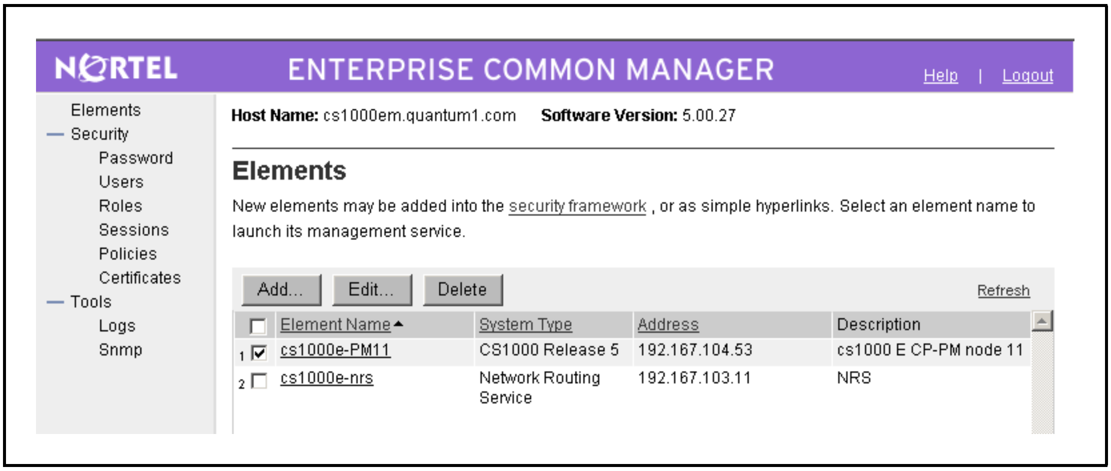
--End--

Change the IPsec PSK on UCM Linux host using Element Manager

If you change the IPsec PSK on the Call Server, you must also change it on the UCM Linux host with Element Manager. For information about changing the IPsec PSK on the Call Server, see .

Procedure 14
Changing the ISSS/IPsec PSK for an IPsec Target that is a CS 1000 component on UCM Linux host using Element Manager

Step	Action
1	Log on to UCM using an account that has the SecurityAdministr ator privilege.
2	On the **Elements** page, select the check box next to the CS 1000 component for which you want to change the IPsec PSK.



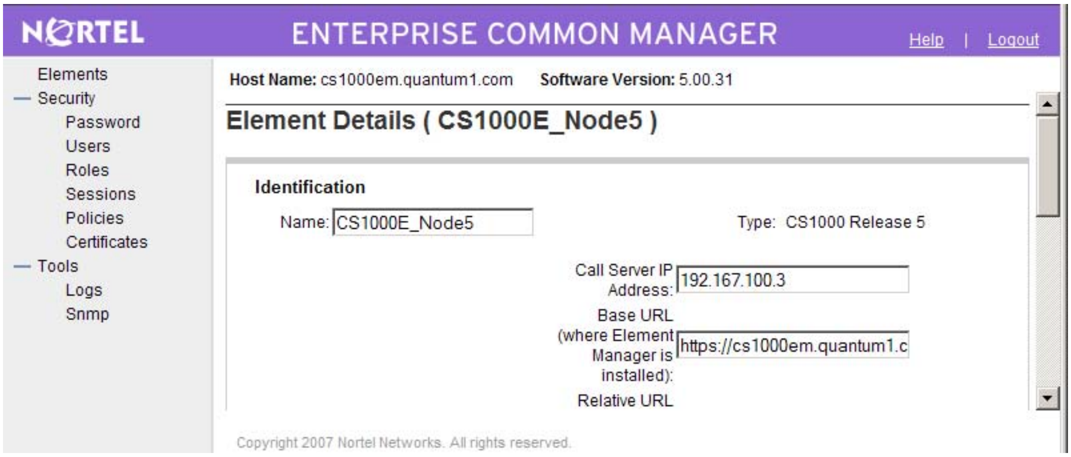
Host Name: cs1000em.quantum1.com **Software Version:** 5.00.27

Elements

New elements may be added into the security framework , or as simple hyperlinks. Select an element name to launch its management service.

	□	Element Name▲	System Type	Address	Description
1	☑	cs1000e-PM11	CS1000 Release 5	192.167.104.53	cs1000 E CP-PM node 11
2	□	cs1000e-nrs	Network Routing Service	192.167.103.11	NRS

Step	Action
3	Click **Edit**. The Element Details page appears.



Host Name: cs1000em.quantum1.com **Software Version:** 5.00.31

Element Details (CS1000E_Node5)

Identification

Name: CS1000E_Node5

Type: CS1000 Release 5

Call Server IP Address: 192.167.100.3

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

Relative URL

Copyright 2007 Nortel Networks. All rights reserved.

4 In the Identification pane, enter the new IPsec PSK in the IPsec Pre-shared Key field, and reenter it in the Confirm IPsec Pre-shared Key field.

5 Click **Save**.

The **Elements** page appears.

6 Click on the name of the component for which you changed the key. Element Manager appears, and automatically updates the IPsec PSK for the IP addresses in the IPsec security policy database.

--End--

Manual ISSS configuration on each device

Use the CLI commands described in the following procedures to configure ISSS settings on individual devices.

CAUTION
Perform the procedures in this section only if you are a security administrator. Nortel recommends that you limit the number of users with security administration privileges.

Configure ISSS targets on a local device

ISSS targets are automatically created on the following devices:

- Voice Gateway Media Card
- MGC
- Signaling Server
- Call Server

Use the following procedure to manually create an ISSS target for devices, such as UCM, so they can encrypt traffic using ISSS.

Procedure 15
Creating a new ISSS target on a local device by using CLI

Step	Action
1	Log on to the OAM (for Signaling Server and MGC) or IPL (for Voice Gateway Media Card) shell using a PWD2 account.
2	Enter the command **`isecNewTarget <IP ADDRESS>`**.

The following message appears:

```
oam> isecNewTarget 192.157.103.4
Changing the local ISEC configuration can cause a
temporary ELAN outage which would last until all
connected elements share the same configuration.
This would affect established calls and IP based
terminal sessions.  NOTE: If this command is
running on one of the CPU's in a redundant CS the
change is not synchronized with the other core.  Are
you sure you want to continue?
```

3 Enter **`yes`**.

The following message appears:

```
The new target has been added locally.
```

--End--

Table 22
Variable definitions

Variable	Value
<IP ADDRESS>	The IP address of the device for which to create a new target.

Use the following procedure to enable an ISSS target for devices such as CallPilot or Unified Communications Manager (UCM).

Procedure 16
Enabling an ISSS target on a local device by using CLI

Step	Action
1	Log on to the OAM (for Signaling Server and MGC) or IPL (for Voice Gateway Media Card) shell using a PWD2 account.
2	Enter the command **`isecEnlTarget <IP ADDRESS>`**.

ATTENTION
This command returns an error in the following situations:

- If no IPsec PSK exists, the system returns an error that indicates you must run the CHG ISEC PSK command to configure an IPsec PSK.
- If no security option exists, the system returns an error that indicates you must run the CHG ISEC <OPTI/FULL> command to configure a security option.

A warning message appears.

3 Enter **`yes`**.

--End--

Use the following procedure to disable an ISSS target for devices such as CallPilot or Unified Communications Management.

Procedure 17
Disabling an ISSS target on a local device by using CLI

Step **Action**

1 Log on to the OAM (for Signaling Server and MGC) or IPL (for Voice Gateway Media Card) shell using a PWD2 account.

2 Enter the command **`isecDisTarget <IP ADDRESS>`**.

The following message appears:

```
oam> isecDisTarget 192.167.103.4
Changing the local ISEC configuration can cause a
temporary ELAN outage which would last until all
connected elements share the same configuration.
This would affect established calls and IP based
terminal sessions.  NOTE: If this command is
running on one of the CPU's in a redundant CS the
change is not synchronized with the other core.  Are
you sure you want to continue?
```

3 Enter **`yes`**.

The following message appears:

```
The target has been disabled.
```

--End--

Use the following procedure to delete an ISSS target for devices such as CallPilot or Unified Communications Management.

Procedure 18
Deleting an ISSS target on a local device by using CLI

Step	Action
1	Log on to the OAM (for Signaling Server and MGC) or IPL (for Voice Gateway Media Card) shell using a PWD2 account.

2	Enter the command **`isecOutTarget <IP ADDRESS>`**.
	The following message appears:
	`oam> isecOutTarget 192.167.103.4`
	`Changing the local ISEC configuration can cause a temporary ELAN outage which would last until all connected elements share the same configuration. This would affect established calls and IP based terminal sessions. NOTE: If this command is running on one of the CPU's in a redundant CS the change is not synchronized with the other core. Are you sure you want to continue?`

3	Enter **`yes`**. The following message appears: `The target has been deleted locally.`

--End--

ATTENTION
Each device must use the same IPsec PSK and ISSS/IPsec security configuration settings as the Call Server. To compare the IPsec PSK and Call Server configuration to that of another device, see .

Certificate Management

This chapter contains procedures to help you manage certificate authorities (CA) and public-key certificates for Secure Socket Layer for Web connections (Web SSL), Datagram Transport Layer Security (DTLS), and Transport Layer Security for Session Initiation Protocol (SIP TLS). The chapter is divided into the following sections:

- "Prepare the system for certificate management" (page 95)
- "CA management" (page 96)
- "Certificate creation and management" (page 103)

The information in this chapter applies to certificate management tools available in Unified Communications Management (UCM) and Element Manager. For information about other tools available in UCM, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

For more information about public-key and private-key certificate concepts, Web SSL, and SIP TLS on Communication Server 1000, see "Public-key certificate concepts" (page 25).

You must log on to the primary security server to perform many of the procedures in this chapter. If the primary security server does not respond, and a backup security server is installed, switch to the backup security server. For more information about switching to the backup security server, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Prepare the system for certificate management

The certificate management procedures in this chapter are performed on Communication Server 1000 system elements.

Nortel recommends that you perform certificate management from the Unified Communications Management primary security server that is running Element Manager. For certificate management purposes, the Unified Communications Management element management table must contain an entry for each Communication Server 1000 system and Signaling Server. You must add the Communication Server 1000 elements and configure ISSS before you perform certificate management. For more information about adding system elements and configuring ISSS, see "IPsec configuration" (page 74). You must also add each Communication Server 1000 system to the Unified Communications Management elements table, and add each signaling server as separate elements.

CA management

Use the information in this section to manage certificate authorities (CA) for SIP TLS. A CA is not needed for Web SSL certificates.

Private CA Configuration

The private CA is generated during installation of the Communication Server 1000 Element Manager and the Network Routing Service (NRS) elements. Once the private CA is generated, you cannot change it. Therefore, during installation you must enter configuration information for the private CA on the primary security server.

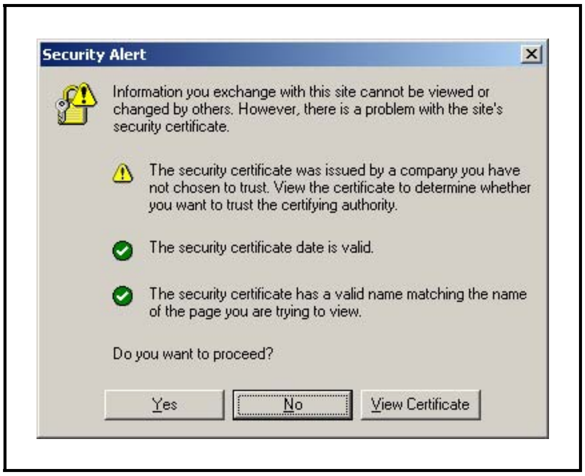
For more information about installing the Communication Server 1000 applications, including the procedure for creating a private CA and configuring SSH trust, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

During the primary security service installation, a Web SSL certificate is issued from the private CA that is installed as part of the primary security service. Use that certificate for the Unified Communications Management Web server, the Sun Access Manager Web server, and the LDAP server.

Use the following procedure to access the primary security server.

Procedure 19
Accessing UCM on the primary security server

Step	Action
1	In the Web browser address field, type **https://<fqdn>**, where <fqdn> is the fully qualified domain name of the primary security server. If the certificate is not installed in the Web browser, a Security Alert window appears, stating that the private CA installed on the primary security server is not in the trusted CA list in the Web browser.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

2 If the CA is not in the trusted list Security Alert window appears, add the private CA to the trusted CA list in the Web browser using Procedure 21 “Installing a certificate into the trusted CA list in the Web browser” (page 98).

3 Click **Yes** to proceed.

--End--

Use the following procedure to view the details of the private CA.

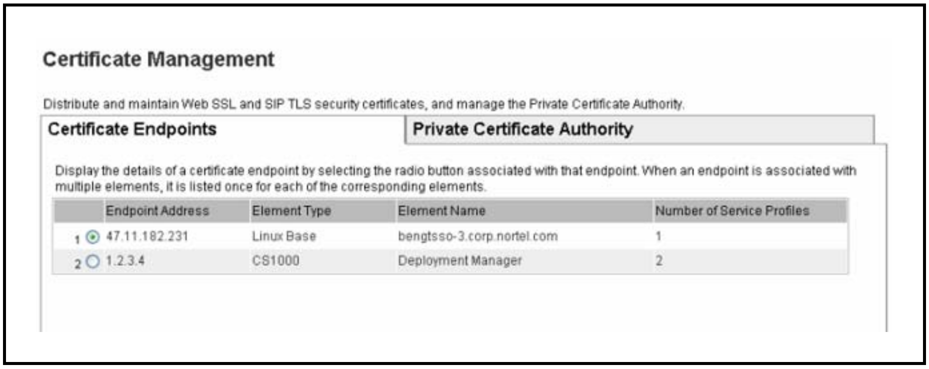
Procedure 20
Viewing private CA details

Step **Action**

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

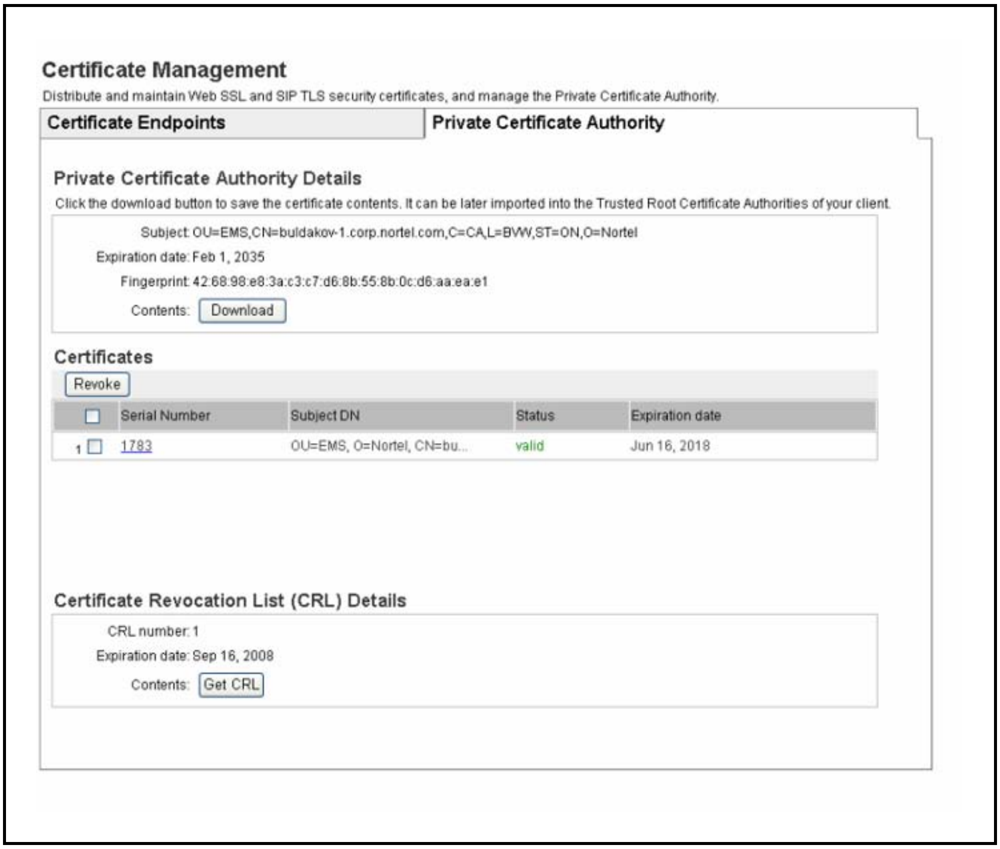
Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

3 Click the **Private Certificate Authority** tab.

The **Private Certificate Authority Details** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Private Certificate Authority Details

Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities of your client.

Subject: OU=EMS,CN=buldakov-1.corp.nortel.com,C=CA,L=BVW,ST=ON,O=Nortel

Expiration date: Feb 1, 2035

Fingerprint: 42:68:98:e8:3a:c3:c7:d6:8b:55:8b:0c:d6:aa:ea:e1

Contents: Download

Certificates

	☐	Serial Number	Subject DN	Status	Expiration date
1	☐	1783	OU=EMS, O=Nortel, CN=bu...	valid	Jun 16, 2018

Certificate Revocation List (CRL) Details

CRL number: 1

Expiration date: Sep 16, 2008

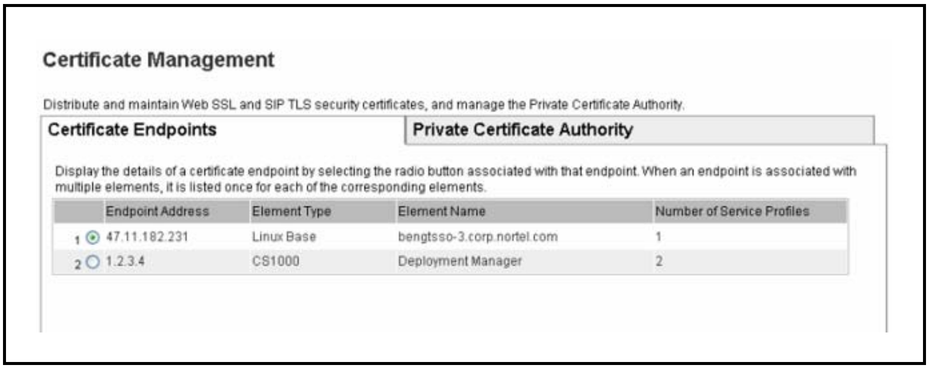
Contents: Get CRL

--End--

Use the following procedure to add the private CA to the trusted CA list in the Web browser.

Procedure 21
Installing a certificate into the trusted CA list in the Web browser

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

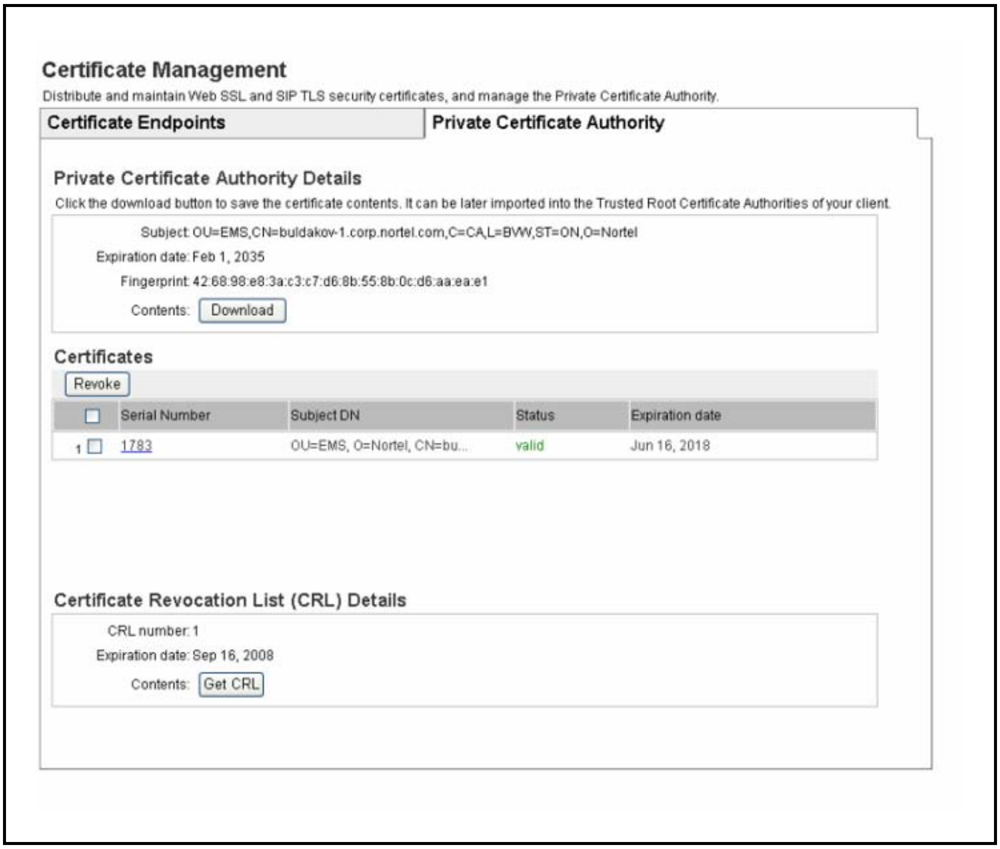
Certificate Endpoints | Private Certificate Authority

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

3 Click the **Private Certificate Authority** tab.

The **Private Certificate Authority Details** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints | Private Certificate Authority

Private Certificate Authority Details

Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities of your client.

Subject: OU=EMS,CN=buldakov-1.corp.nortel.com,C=CA,L=BVW,ST=ON,O=Nortel

Expiration date: Feb 1, 2035

Fingerprint: 42:68:98:e8:3a:c3:c7:d6:8b:55:8b:0c:d6:aa:ea:e1

Contents: Download

Certificates

Revoke

	Serial Number	Subject DN	Status	Expiration date
□				
1 □	1783	OU=EMS, O=Nortel, CN=bu...	valid	Jun 16, 2018

Certificate Revocation List (CRL) Details

CRL number: 1

Expiration date: Sep 16, 2008

Contents: Get CRL

4 Click **Download** to download the certificate.

5 Follow the prompts in the wizard to install the certificate into the trusted CA list of the Web browser.

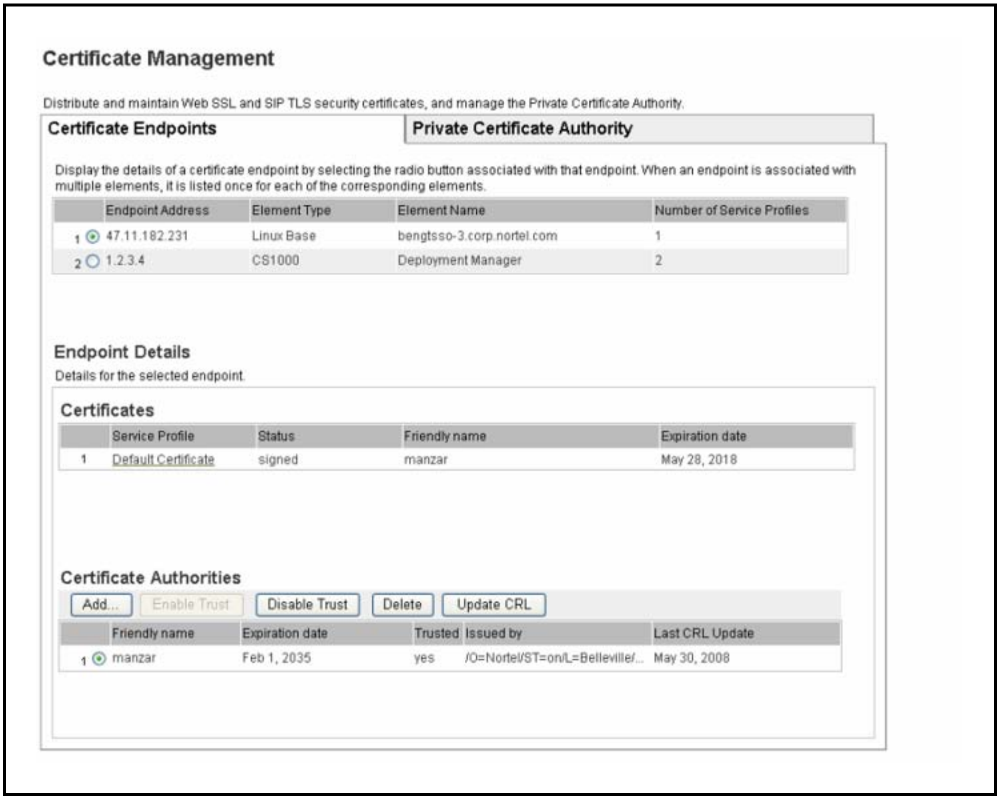
--End--

Add a CA to an endpoint

Use the following procedure to add a CA to a selected endpoint by using Unified Communications Management.

Procedure 22
Adding a CA to an endpoint

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

Endpoint Details

Details for the selected endpoint.

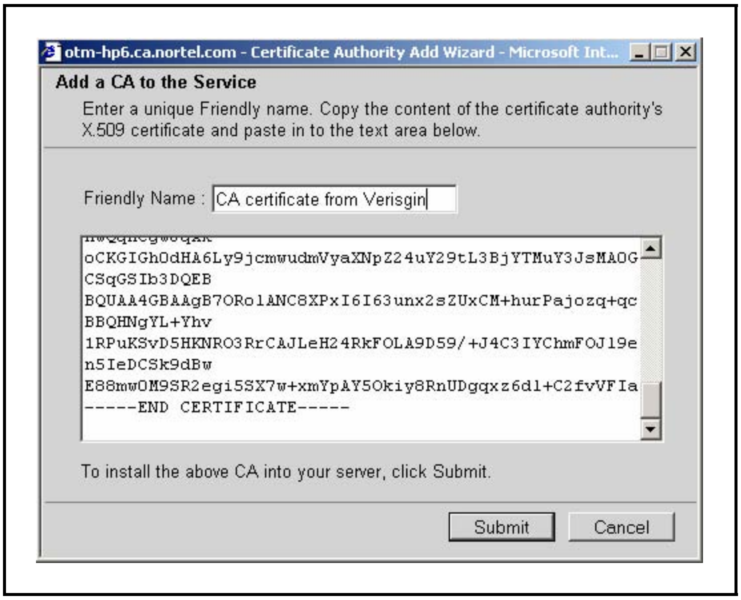
Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	manzar	May 28, 2018

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ●	manzar	Feb 1, 2035	yes	/O=Nortel/ST=on/L=Belleville/...	May 30, 2008

Step	Action
3	In the **Certificate Endpoints** pane, select the radio button next to an endpoint.
4	In the **Certificate Authorities** pane, click **Add**. The **Add a CA to the Service** window appears.



otm-hp6.ca.nortel.com - Certificate Authority Add Wizard - Microsoft Int...

Add a CA to the Service

Enter a unique Friendly name. Copy the content of the certificate authority's X.509 certificate and paste in to the text area below.

Friendly Name : CA certificate from Verisgin

```
oCKGIGh0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA0G
CSqGSIb3DQEB
BQUAA4GBAAgB7ORolANC8XPxI6I63unx2sZUxCM+hurPajozq+qc
BBQHNgYL+Yhv
1RPuKSvD5HKNRO3RrCAJLeH24RkFOLA9D59/+J4C3IYChmFOJl9e
n5IeDCSk9dBw
E88mwOM9SR2egi5SX7w+xmYpAY5Okiy8RnUDgqxz6dl+C2fvVFIa
-----END CERTIFICATE-----
```

To install the above CA into your server, click Submit.

5 Type a name in the **Friendly Name** field.

6 Copy the contents of the X.509 certificate, which is provided by the CA in a privacy-enhanced electronic mail (PEM) text file.

7 In the **Add a CA to the Service** window, click in the text box, and press **ctrl-v** to paste the certificate text.

8 Click **Submit**.

9 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Change the trust status of an endpoint

Use the following procedure to enable or disable trust for an endpoint.

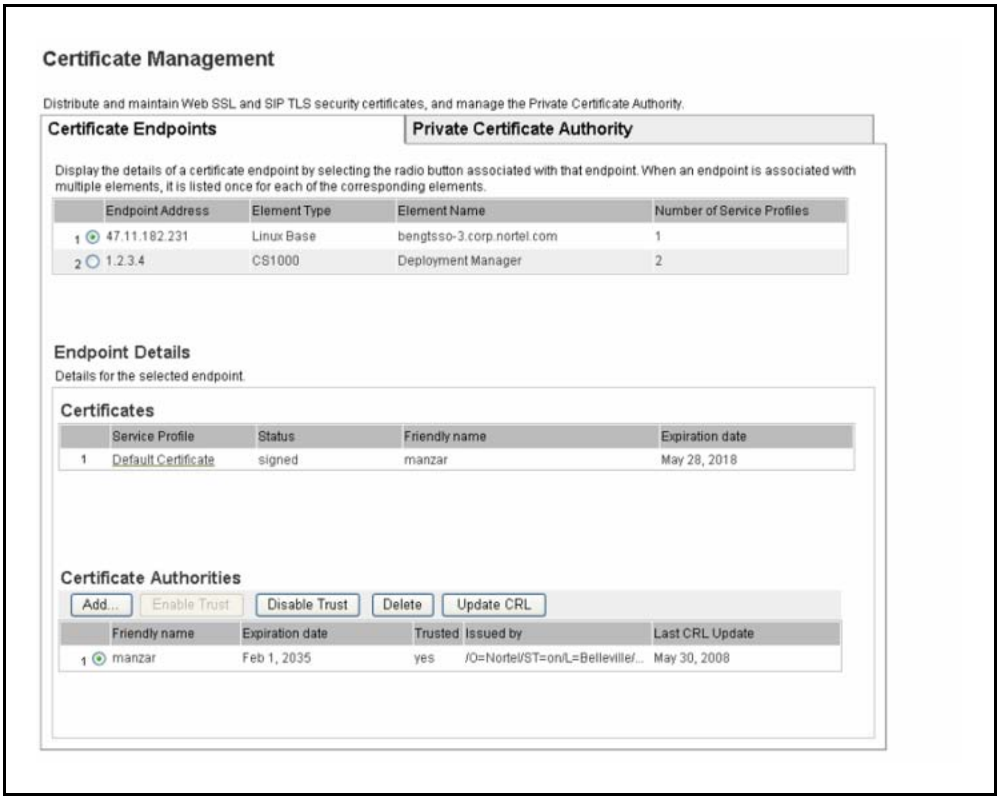
Procedure 23
Changing the trust status of an endpoint certificate

Step **Action**

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	manzar	May 28, 2018

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ●	manzar	Feb 1, 2035	yes	/O=Nortel/ST=on/L=Belleville/...	May 30, 2008

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure.

4 In the **Certificate Authorities** pane, select a CA.

5 In the **Certificate Authorities** pane, click one of:

Enable Trust
OR
Disable Trust .

The modified trust status appears on the page.

6 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Delete a CA

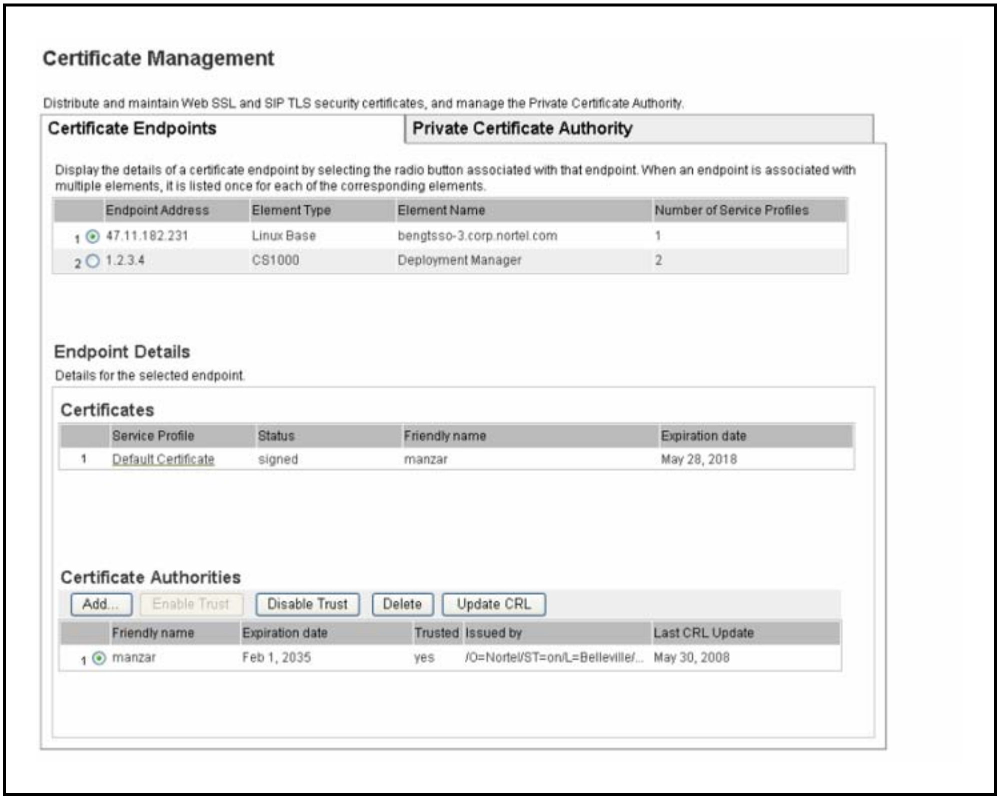
Use the following procedure to delete a CA.

Procedure 24
Deleting a CA

Step	Action
1	Log on to the UCM primary security server using an account that has Security Administrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	manzar	May 28, 2018

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ●	manzar	Feb 1, 2035	yes	/O=Nortel/ST=on/L=Belleville/...	May 30, 2008

3 In the **Certificate Endpoints** pane, select the radio button next to an endpoint.

4 In the **Certificate Authorities** pane, select a CA.

5 Click **Delete**. A confirmation window appears.

6 Click **OK**.

7 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Certificate creation and management

Use the procedures in this section to view the certificate details for an endpoint, or to configure Web SSL and SIP TLS certificates for endpoints.

You can use the Unified Communications Management Certificate Management Wizard to complete the tasks listed in Table 23 "Certificate Management Wizard configuration options" (page 104).

Table 23
Certificate Management Wizard configuration options

create a new certificate signed by a local private CA
import a certificate and its private key from a file
assign an existing certificate
create a new self-signed certificate
create a new certificate request to be signed by a third-party CA
process a pending certificate response
delete a pending certificate response
export the current self-signed certificate
export the current certificate and its private key
replace the current certificate
remove the current certificate
create a certificate renew request for the current certificate

ATTENTION
If you use Unified Communications Management to configure a certificate for an endpoint that is behind a firewall, open port 22 to allow SSH to communicate with the endpoint.

For more information about the different status types for Web SSL and SIP TLS certificates, see Table 24 "Status types for certificate endpoints" (page 104).

Table 24
Status types for certificate endpoints

Status type	Description
unknown	The certificate endpoint cannot be reached.
none	No X.509 certificate is issued for the service of the endpoint.
self-signed	A self-signed X.509 certificate is issued for the service of the endpoint.
pending	An X.509 certificate request is created for the service of the endpoint. The certificate request must be signed by a CA.
signed	An X.509 certificate signed by a CA is issued for the service of the endpoint.
pending renew	An X.509 certificate signed by a CA is issued for the service of the endpoint. A certificate renew request is created for the service. The certificate renew request must be signed by a CA.

Table 24
Status types for certificate endpoints (cont'd.)

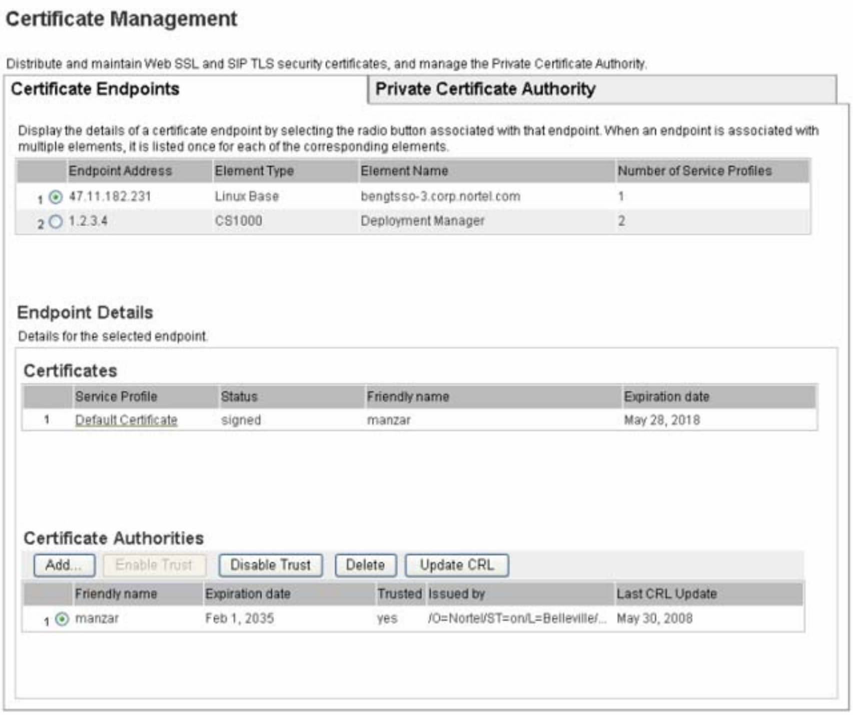
Status type	Description
about to expire	An X.509 certificate signed by a CA is issued for the service of the endpoint. The certificate will expire in less than 60 days.
expired	An X.509 certificate signed by a CA is issued for the service of the endpoint. The certificate has expired.

Certificate information

Use the following procedure to view the details about certificate endpoints and CAs.

Procedure 25
Viewing certificate details for an endpoint by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	manzar	May 28, 2018

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ●	manzar	Feb 1, 2035	yes	/O=Nortel/ST=on/L=Belleville/...	May 30, 2008

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to view.

The **Endpoint Details** section displays the details for the selected endpoint.

For more information about the different status types, see Table 24 "Status types for certificate endpoints" (page 104).

--End--

Add a UCM server certificate to the Web browser

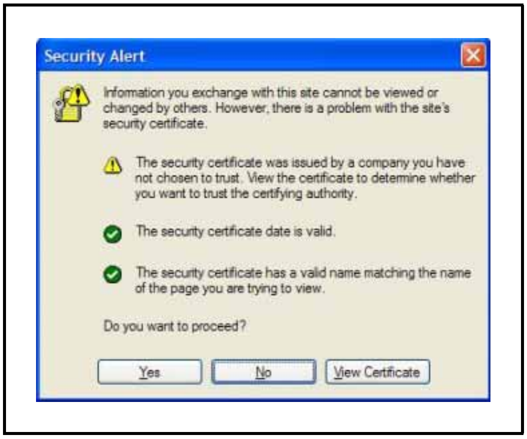
When visiting a UCM server using a Web browser for the first time, a warning box (Security Alert) appears regarding a problem with the authenticity of the server certificate. The server certificate can be trusted; however, this warning appears each time you visit the site.

Use this procedure to add the UCM server certificate to the Web browser as a trusted certificate. This prevents the warning from appearing each time you visit the site.

Procedure 26
Adding a UCM server certificate to the Web browser

Step	Action

1 When the following Security Alert appears, click **View Certificate**.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

The certificate information displays.

2 Click the **Certification Path** tab.

3 In the Certification Path view, select the root CA certificate.

The CA certificate is represented at the top of the hierarchy. It normally has a red check mark beside it to indicate that it is not yet trusted.

4 Click **View Certificate**.

The details of the root CA certificate are displayed.

5 Click **Install Certificate**.

The installation wizard appears.

6 Click **Next** for each screen to accept the defaults.

7 Click **Yes** to install the certificate.

The browser now trusts all certificates within the UCM security domain.

To confirm, you can view your browsers trusted CA list by doing the following:

- For Microsoft Internet Explorer 6.0, select **Tools** > **Internet Options**.
- Select the **Content** tab.
- Click **Certificates**.
- Select the **Trusted Root Certificate Authorities** tab.
- Scroll down to view the entry for the Private CA certificate. Its name should match the FQDN of the UCM primary security server.

--End--

Create a certificate for Web SSL signed by the private CA

Use the following procedure to create a new certificate request that is signed by a private CA.

Prerequisites

- Before you create a new certificate signed by a local private CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

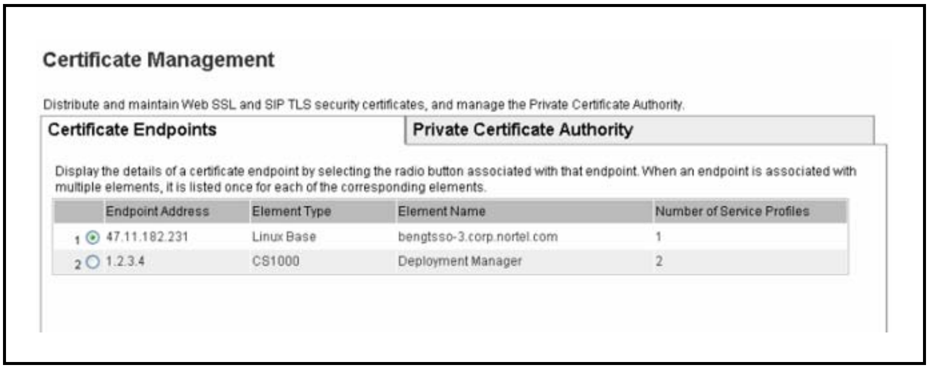
Procedure 27
Creating a certificate for Web SSL signed by the private CA

Step **Action**

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

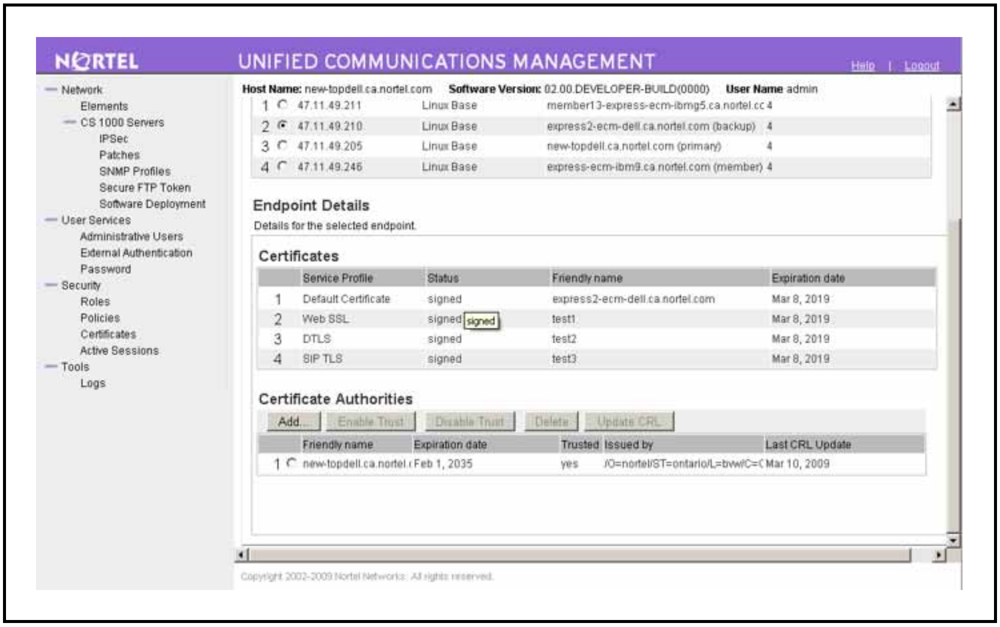
Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

3 In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

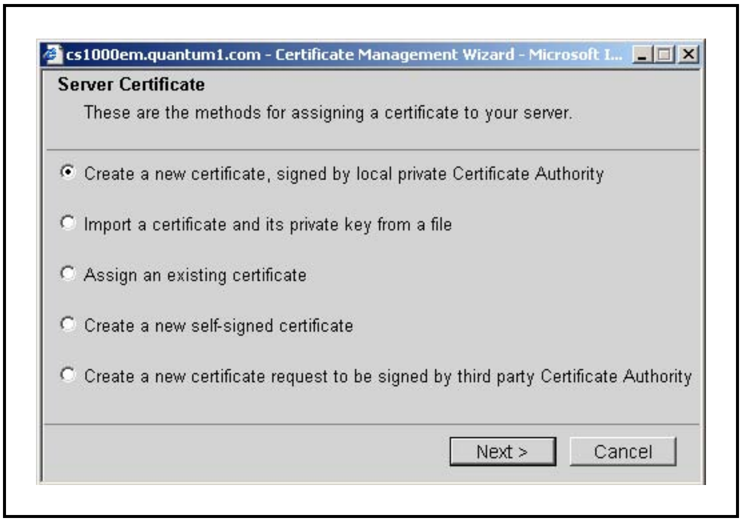
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

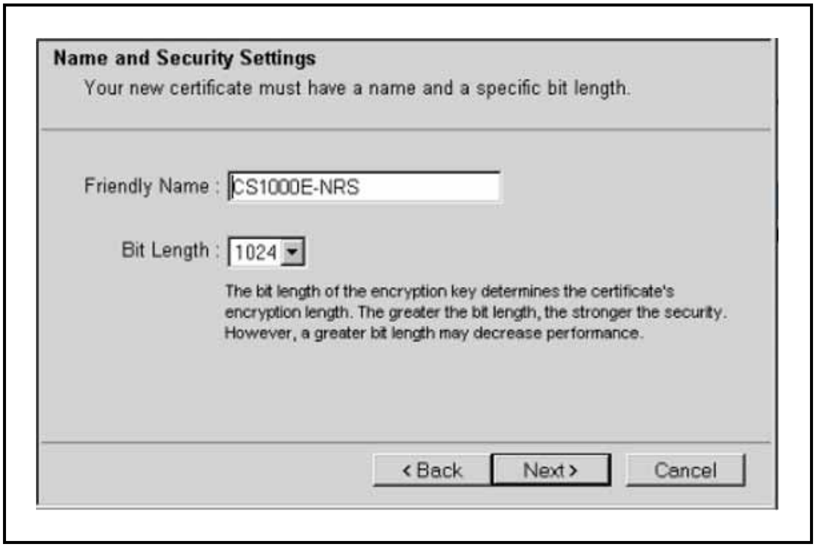
○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Create a new certificate, signed by local private Certificate Authority** and click **Next**.

The **Name and Security Settings** window appears.


Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

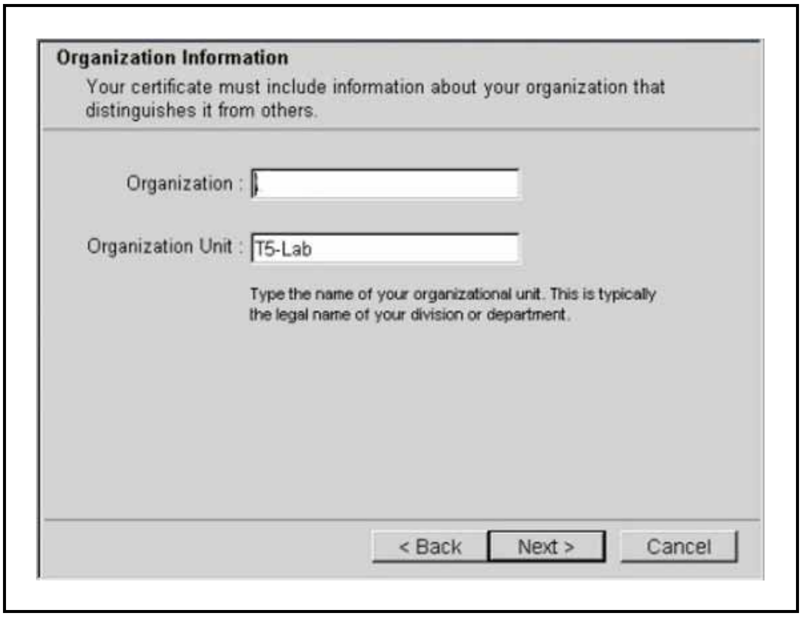
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

6 Type a name in the **Friendly Name** field.

7 Select a bit length from the **Bit length** list.

8 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

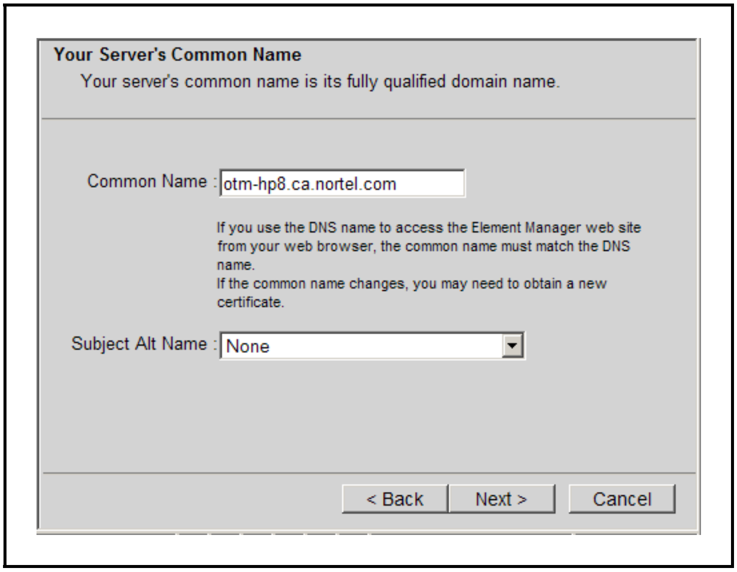
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

9 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

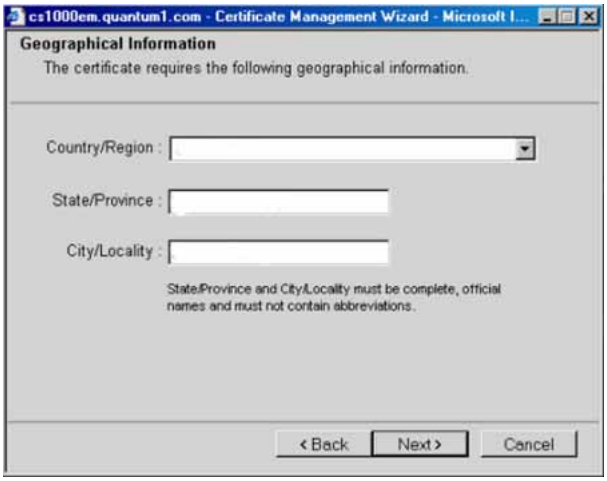
Subject Alt Name : None

10 In the **Common Name** field, enter the fully qualified domain name (FQDN) of the server you are configuring.

The **Subject Alt Name** field must be selected as None.

11 Click **Next**.

The **Geographical Information** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Country/Region :
State/Province :
City/Locality :
< Back
Next >
Cancel

Geographical Information

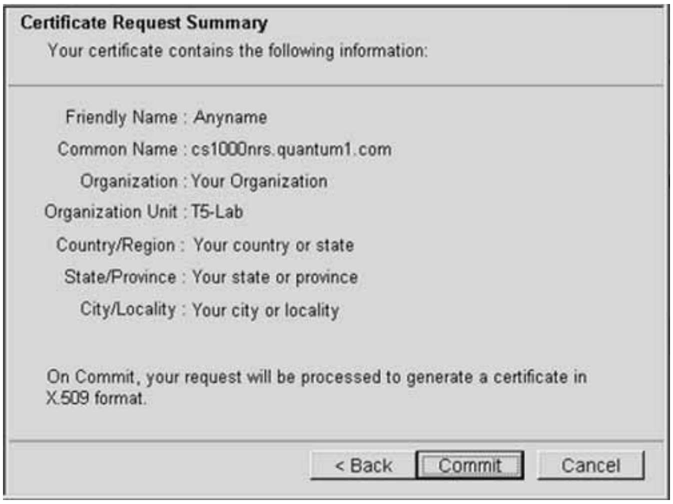
The certificate requires the following geographical information.

State/Province and City/Locality must be complete, official names and must not contain abbreviations.

12 In the **Geographical Information** window, perform the following tasks:

- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



Certificate Request Summary

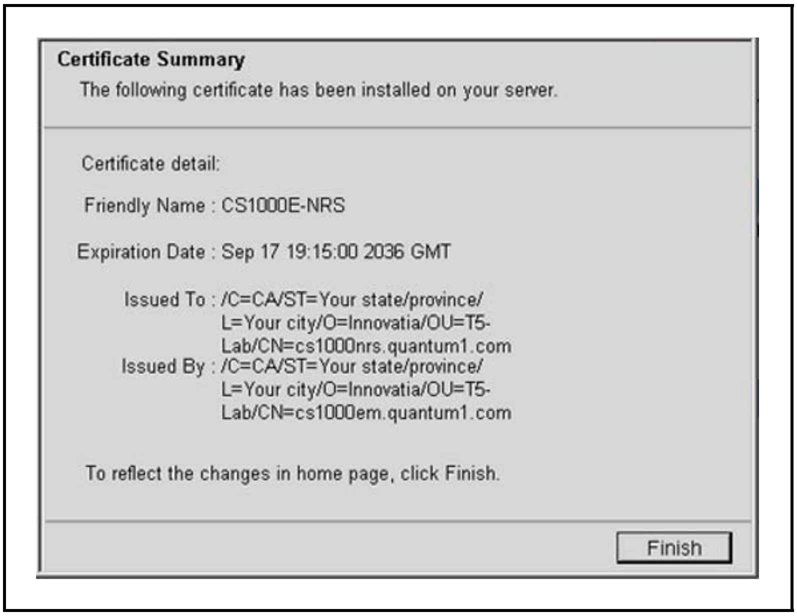
Your certificate contains the following information:

Friendly Name : Anyname
Common Name : cs1000nrs.quantum1.com
Organization : Your Organization
Organization Unit : T5-Lab
Country/Region : Your country or state
State/Province : Your state or province
City/Locality : Your city or locality

On Commit, your request will be processed to generate a certificate in X.509 format.

13 Click **Commit** to generate a certificate in X.509 format.

The **Certificate Summary** window appears with the certificate information.



Certificate Summary

The following certificate has been installed on your server.

Certificate detail:

Friendly Name : CS1000E-NRS

Expiration Date : Sep 17 19:15:00 2036 GMT

Issued To : /C=CA/ST=Your state/province/
L=Your city/O=Innovatia/OU=T5-
Lab/CN=cs1000nrs.quantum1.com

Issued By : /C=CA/ST=Your state/province/
L=Your city/O=Innovatia/OU=T5-
Lab/CN=cs1000em.quantum1.com

To reflect the changes in home page, click Finish.

14 Click **Finish**.

The status changes to signed.

15 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Create a certificate for Web SSL signed by a trusted third-party CA

Use the following procedure to create a new certificate request to be signed by a third-party CA.

Prerequisites

- Before you create a request for a new certificate signed by a third-party CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

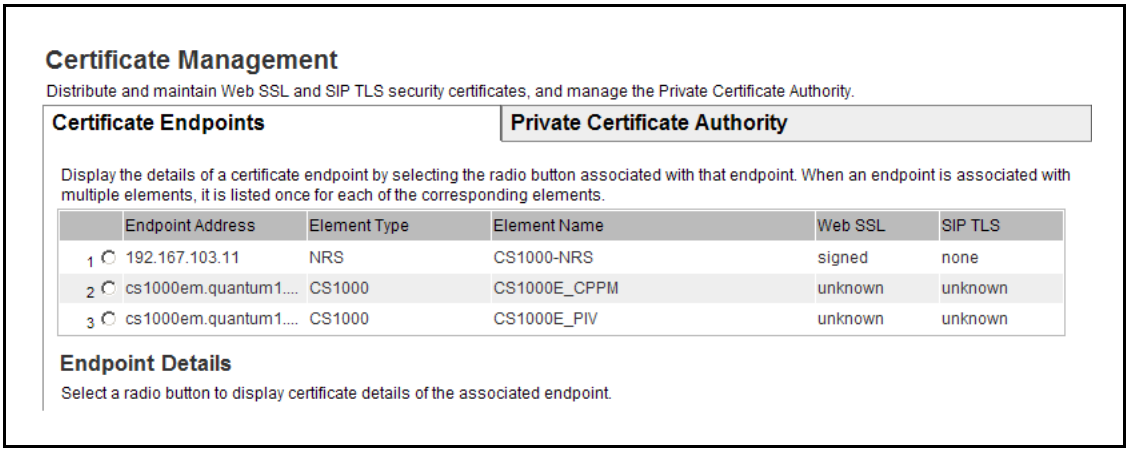
Procedure 28
Creating a request for a certificate for Web SSL signed by third-party CA

Step **Action**

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

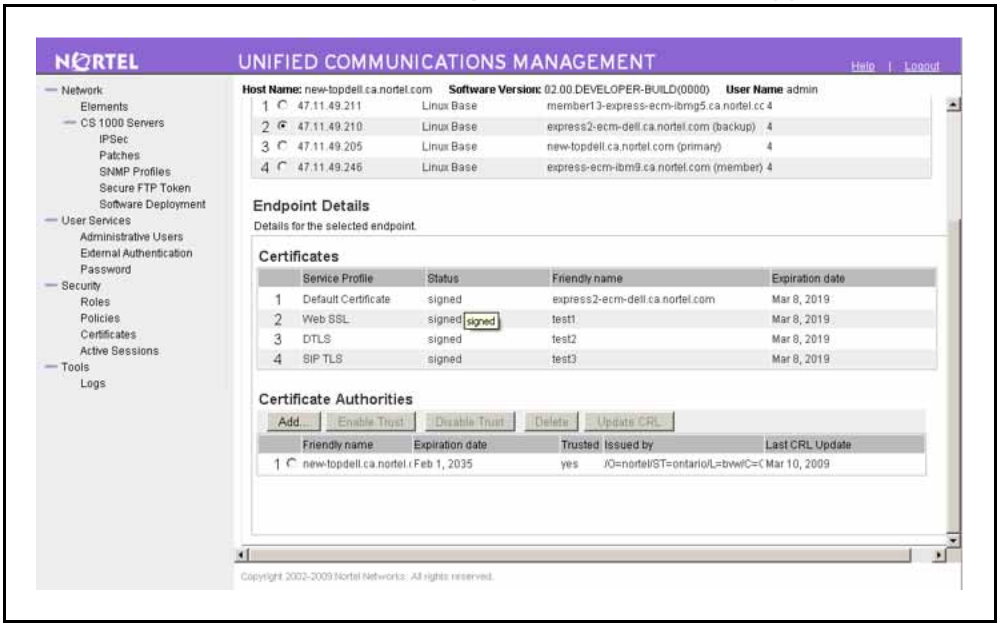
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

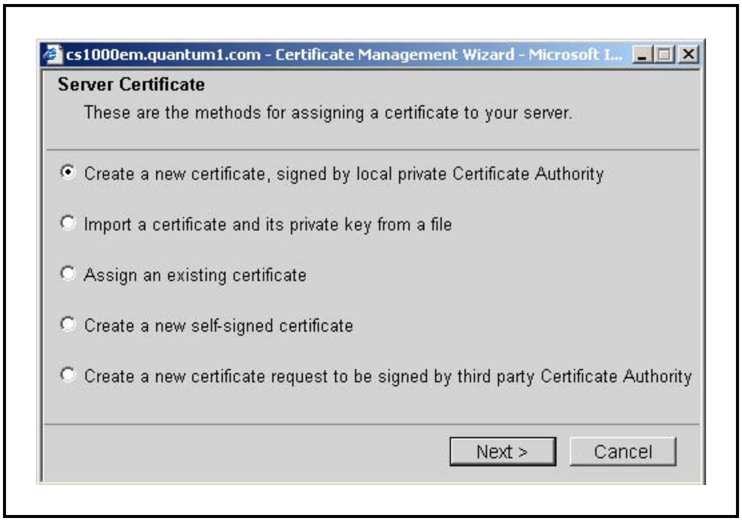
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **Web SSL**.

The **Server Certificate** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

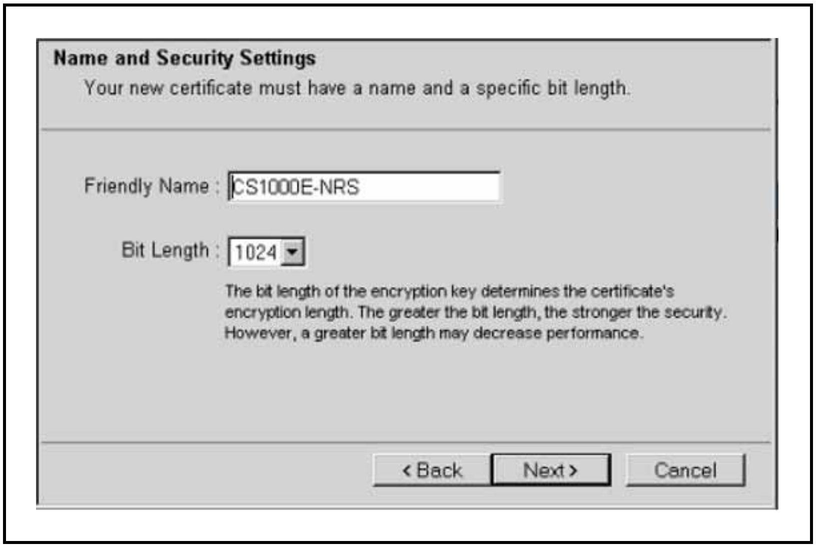
○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Create a new certificate request to be signed by third party** and click **Next**.

The **Name and Security Settings** window appears.



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

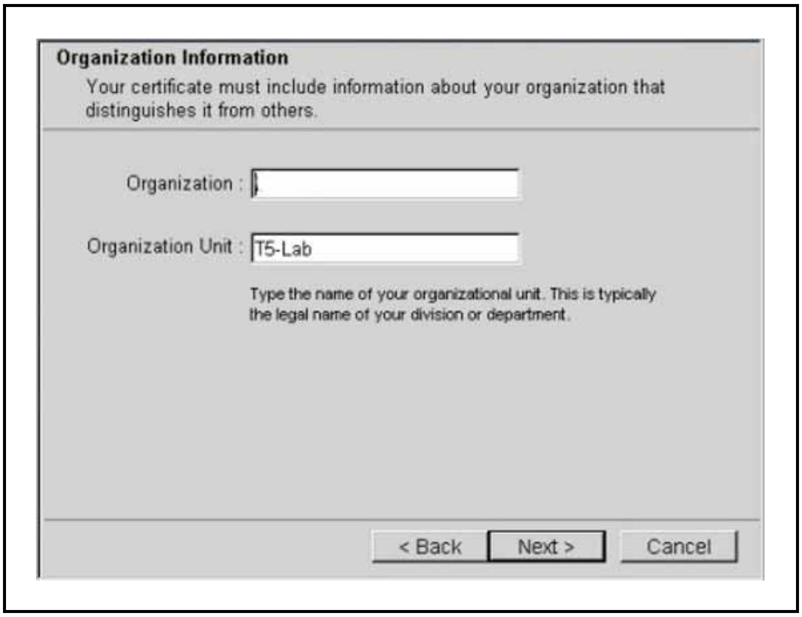
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

6 Type a name in the **Friendly Name** field.

7 Select a bit length from the **Bit length** list.

8 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

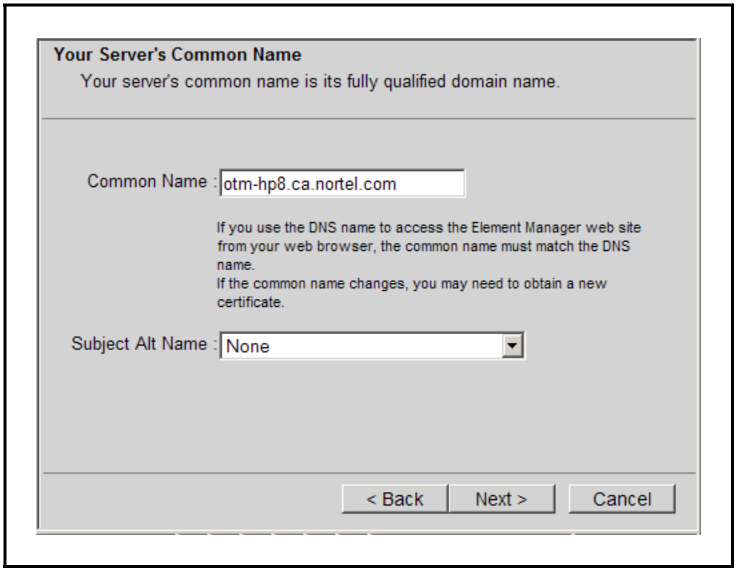
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

9 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name : None

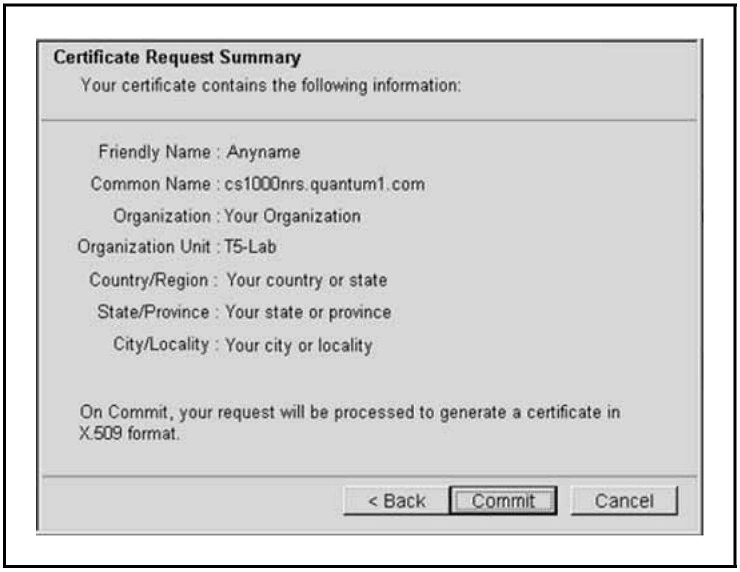
10 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.

11 In the **Geographical Information** , perform the following tasks:

- Enter a **Country/Region**.
- Enter a **State/Province**.
- Enter a **City/Locality**.
- Click **Next**.

The **Certificate Request Summary** window appears.



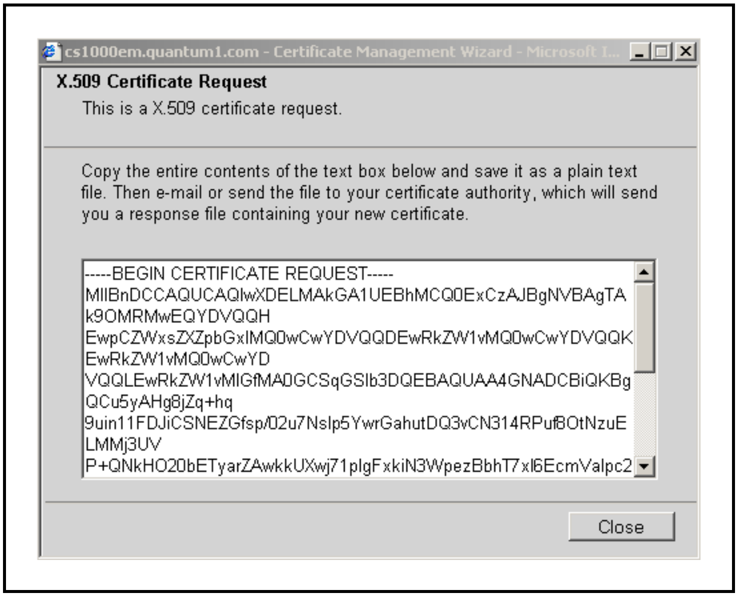
Certificate Request Summary

Your certificate contains the following information:

Friendly Name : Anyname
Common Name : cs1000nrs.quantum1.com
Organization : Your Organization
Organization Unit : T5-Lab
Country/Region : Your country or state
State/Province : Your state or province
City/Locality : Your city or locality

On Commit, your request will be processed to generate a certificate in X.509 format.

12 Click **Commit**. The **X.509 Certificate Request** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

X.509 Certificate Request

This is a X.509 certificate request.

Copy the entire contents of the text box below and save it as a plain text file. Then e-mail or send the file to your certificate authority, which will send you a response file containing your new certificate.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUCAQIwXDELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTA
k9OMRMwEQYDVQQH
EwpCZWxsZXZpbGxlMQ0wCwYDVQQDEwRkZW1vMQ0wCwYDVQQK
EwRkZW1vMQ0wCwYD
VQQLEwRkZW1vMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
QCu5yAHg8jZq+hq
9uin11FDJiCSNEZGfsp/02u7NsIp5YwrGahutDQ3vCN314RPuf8OtNzuE
LMMj3UV
P+QNkHO20bETyarZAwkkUXwj71pIgFxkiN3WpezBbhT7xI6EcmValpc2
```

The X.509 Certificate Request window contains the certificate signing request (CSR).

13 To copy the CSR, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

The status changes to pending.

14 Paste the certificate text into a text editor, and save it in a plain text file.

15 Send the CSR to the third-party CA.

After you receive the signed certificate from the third-party CA, use the following steps to process and install the certificate, and then add the text from the third-party CA.

16 To process the pending request and install the certificate, follow the steps in Procedure 35 “Processing a pending certificate request by using UCM” (page 144).

The status changes to signed.

17 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

After you restart the system, a Security Alert appears. Carry out the following two actions:

- Follow the instructions from the third-party vendor to download the intermediate CA.
- Follow the steps in Procedure 22 “Adding a CA to an endpoint” (page 100) to add the intermediate CA to the browser.

Create a self-signed certificate for Web SSL

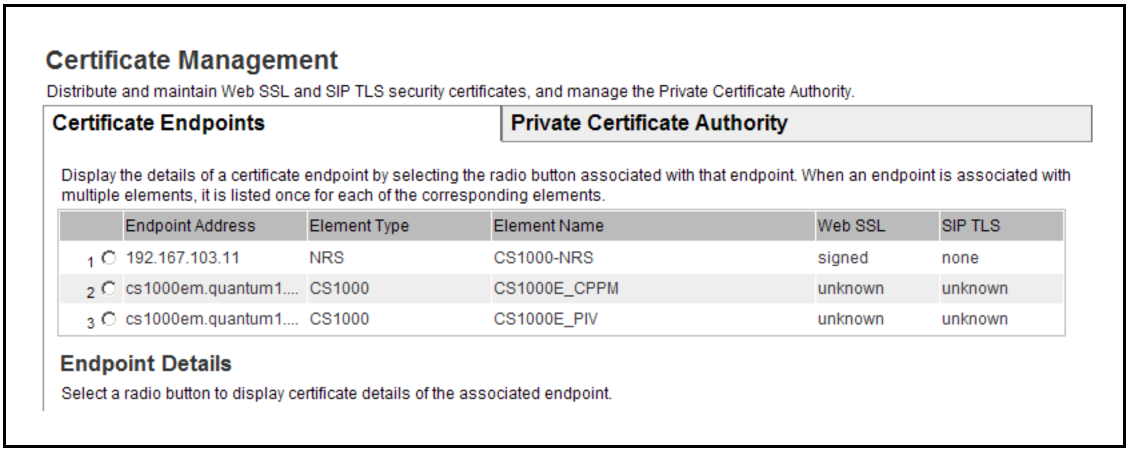
Use the following procedure to create a new self-signed certificate.

Prerequisites

- Before you create a new self-signed certificate, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 29
Creating a self-signed certificate for Web SSL

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

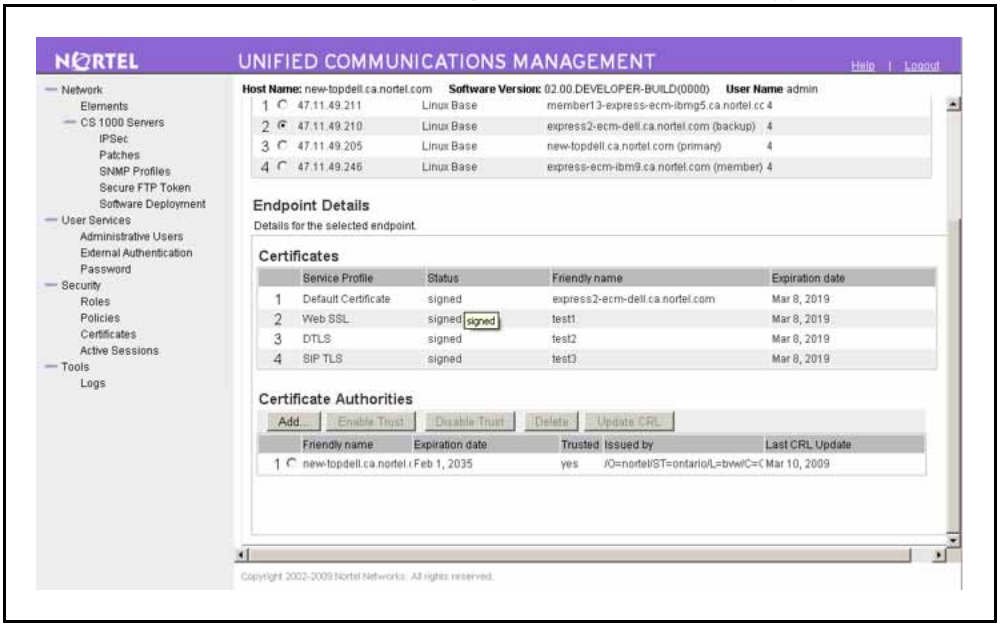
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

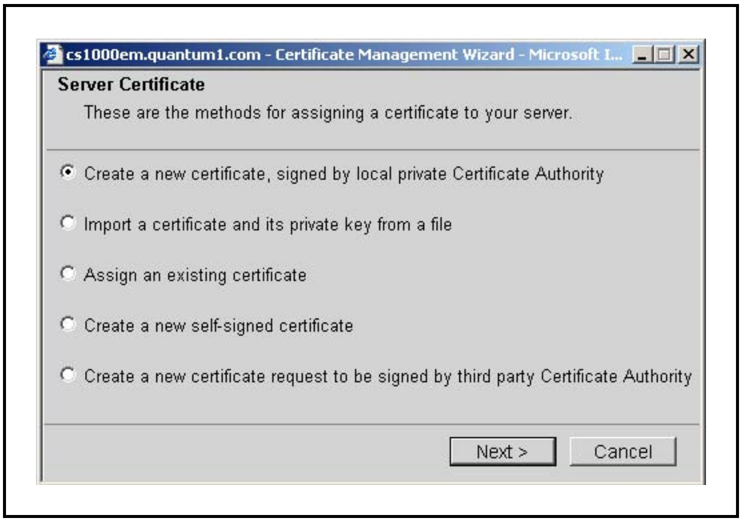
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.c	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

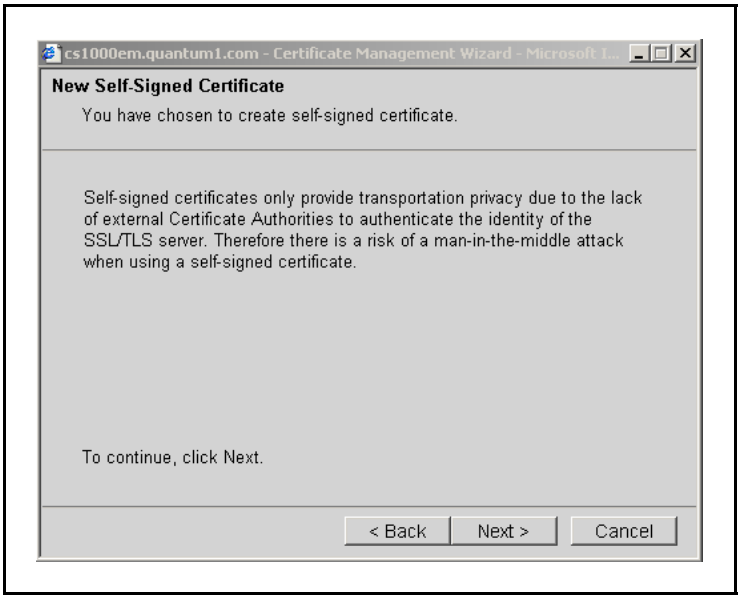
○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Create a new self-signed certificate**, and click **Next**.

The **New Self-Signed Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

New Self-Signed Certificate

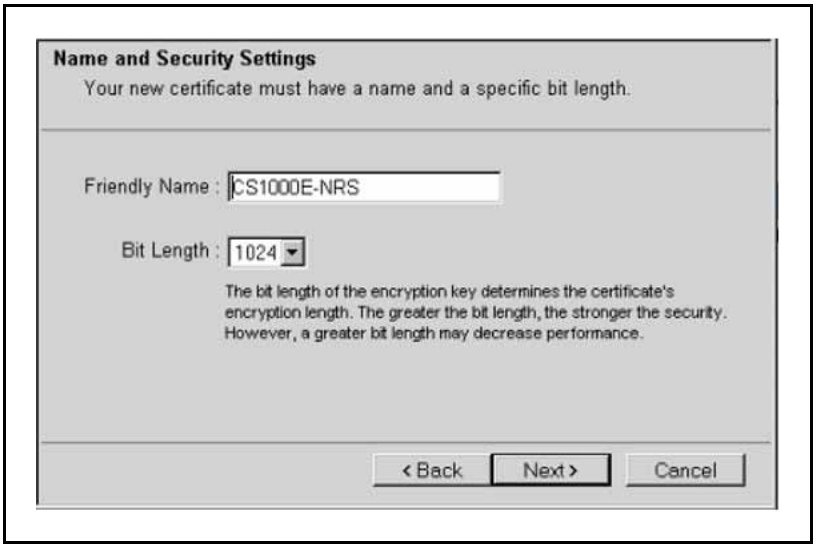
You have chosen to create self-signed certificate.

Self-signed certificates only provide transportation privacy due to the lack of external Certificate Authorities to authenticate the identity of the SSL/TLS server. Therefore there is a risk of a man-in-the-middle attack when using a self-signed certificate.

To continue, click Next.

6 Click **Next**.

The **Name and Security Settings** window appears.



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

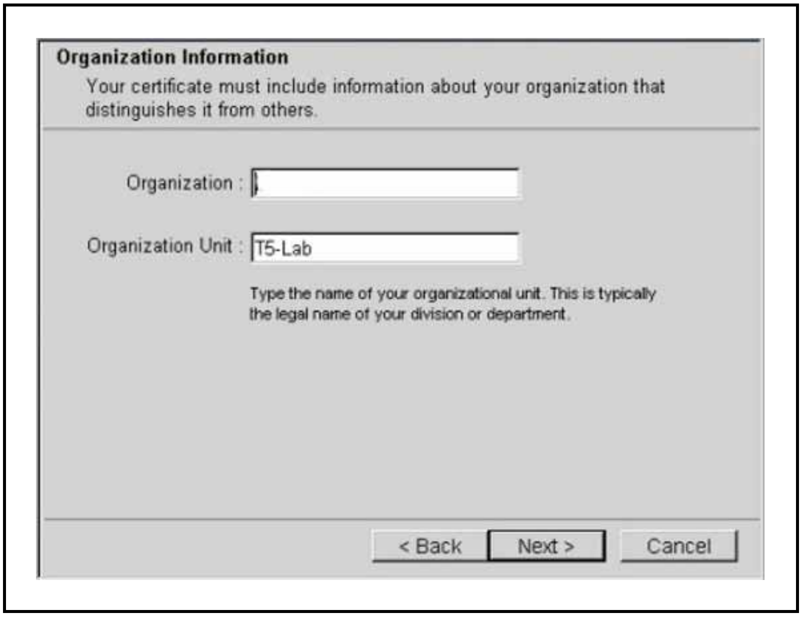
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

7 Type a name in the **Friendly Name** field.

8 Select a bit length from the **Bit length** list.

9 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

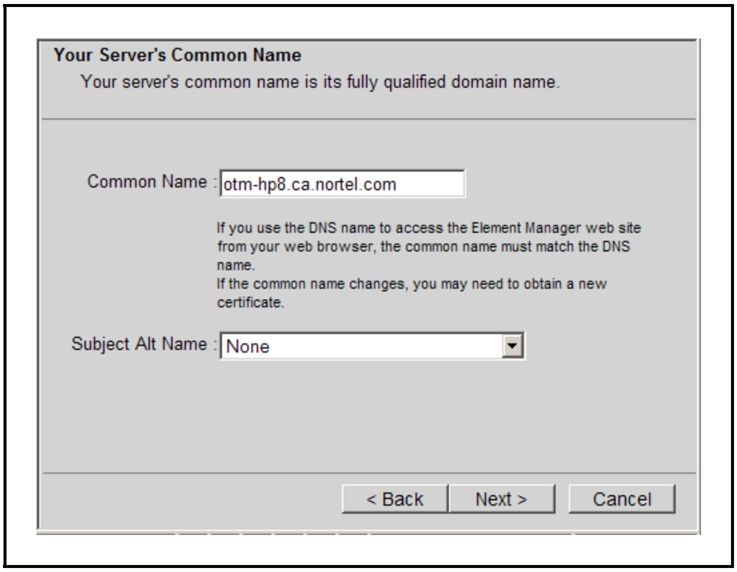
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

10 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

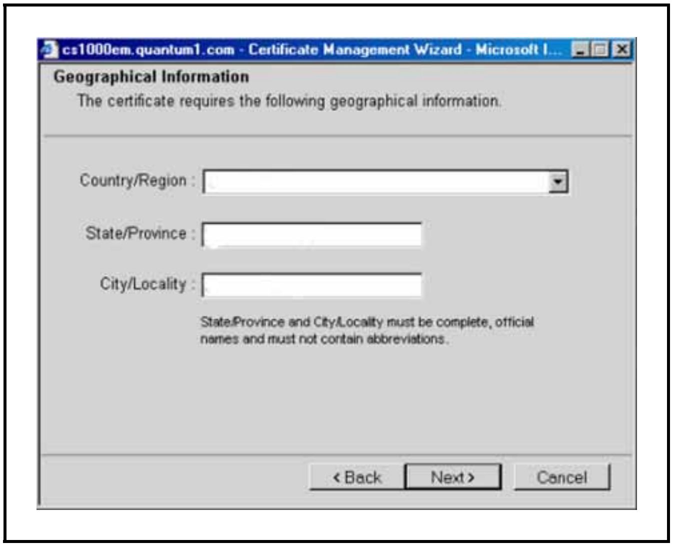
Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name : None

11 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Geographical Information

The certificate requires the following geographical information.

Country/Region :

State/Province :

City/Locality :

State/Province and City/Locality must be complete, official names and must not contain abbreviations.

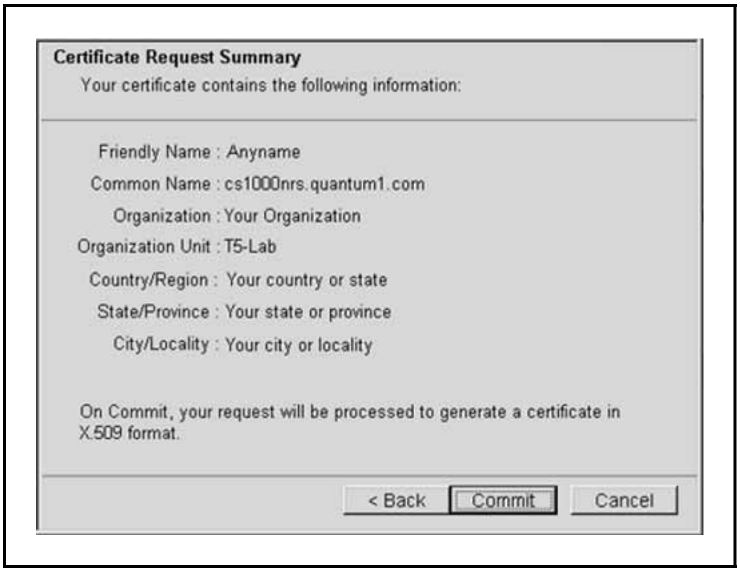
12 Enter a **Country/Region**.

13 Enter a **State/Province**.

14 Enter a **City/Locality**.

15 Click **Next**.

The **Certificate Request Summary** window appears.



Certificate Request Summary

Your certificate contains the following information:

Friendly Name : Anyname

Common Name : cs1000nrs.quantum1.com

Organization : Your Organization

Organization Unit : T5-Lab

Country/Region : Your country or state

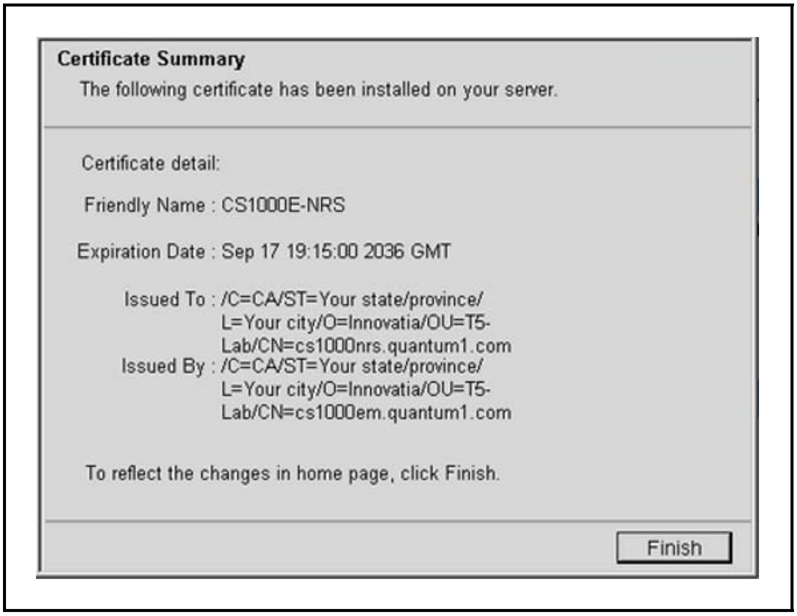
State/Province : Your state or province

City/Locality : Your city or locality

On Commit, your request will be processed to generate a certificate in X.509 format.

16 Click **Commit**.

The **Certificate Summary** window appears.



Certificate Summary

The following certificate has been installed on your server.

Certificate detail:

Friendly Name : CS1000E-NRS

Expiration Date : Sep 17 19:15:00 2036 GMT

Issued To : /C=CA/ST=Your state/province/ L=Your city/O=Innovatia/OU=T5-Lab/CN=cs1000nrs.quantum1.com

Issued By : /C=CA/ST=Your state/province/ L=Your city/O=Innovatia/OU=T5-Lab/CN=cs1000em.quantum1.com

To reflect the changes in home page, click Finish.

17 Click **Finish**.

The status changes to self-signed.

18 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

After you restart the system, a Security Alert appears. Carry out the following two actions:

- Follow the steps in Procedure 38 “Exporting the current self-signed certificate by using UCM” (page 151) to export the self-signed certificate.
- Follow the steps in Procedure 22 “Adding a CA to an endpoint” (page 100) to add the self-signed certificate into the trusted CA list for the web browser.

Create a certificate for SIP TLS signed by the private CA

Use the following procedure to create a new certificate request that is signed by a private CA.

Prerequisites

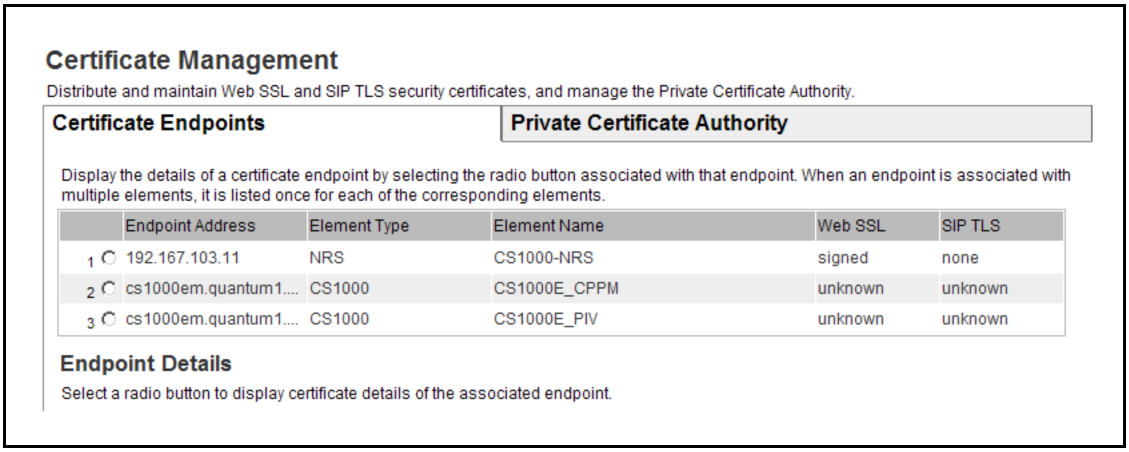
- Before you create a request for a new certificate signed by a local CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 30
Creating a certificate for SIP TLS signed by the private CA

Step **Action**

1 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

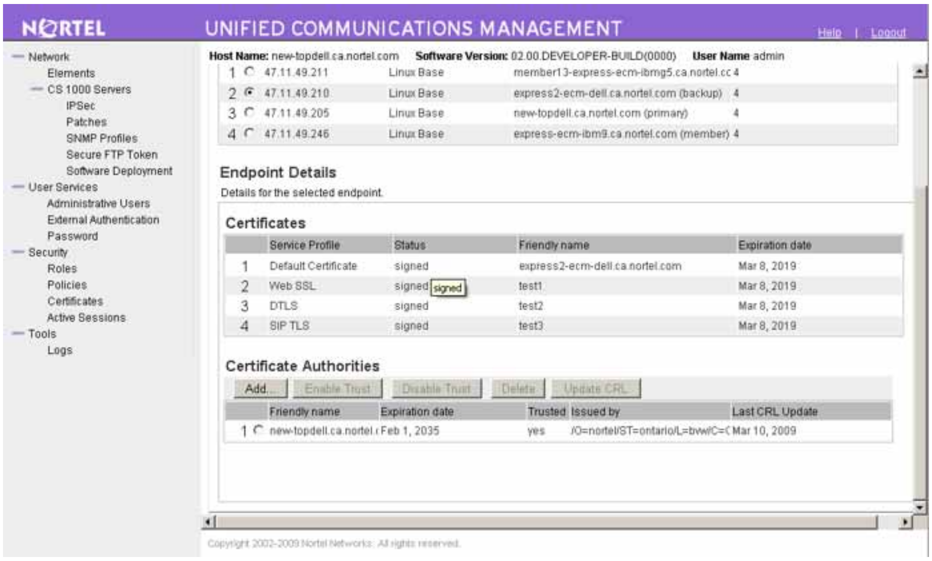
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

2 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

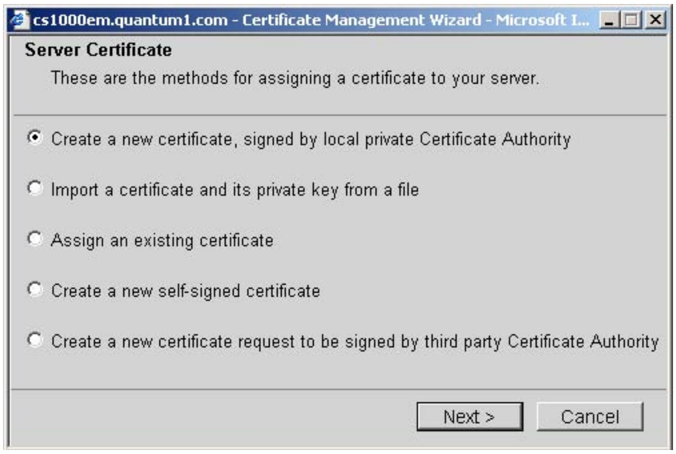
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

3 In the Endpoint Details pane, under Certificates, click **SIP TLS**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Next >
Cancel

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

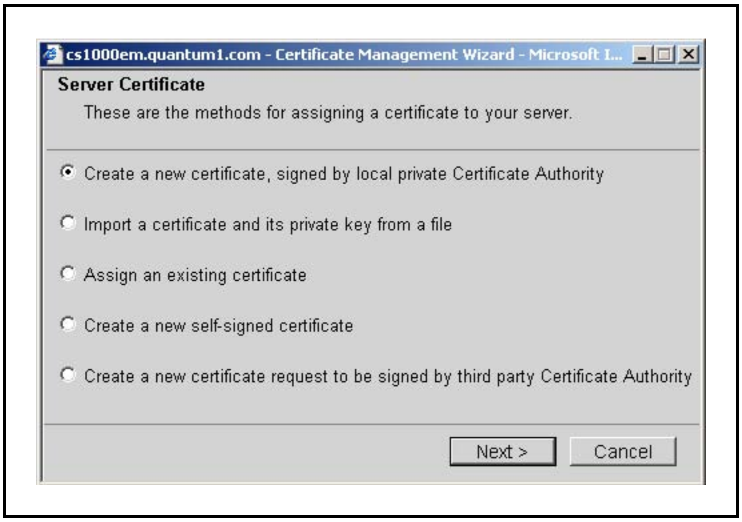
○ Import a certificate and its private key from a file

○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

4 Select **Create a new certificate, signed by local private Certificate Authority** and click **Next**.



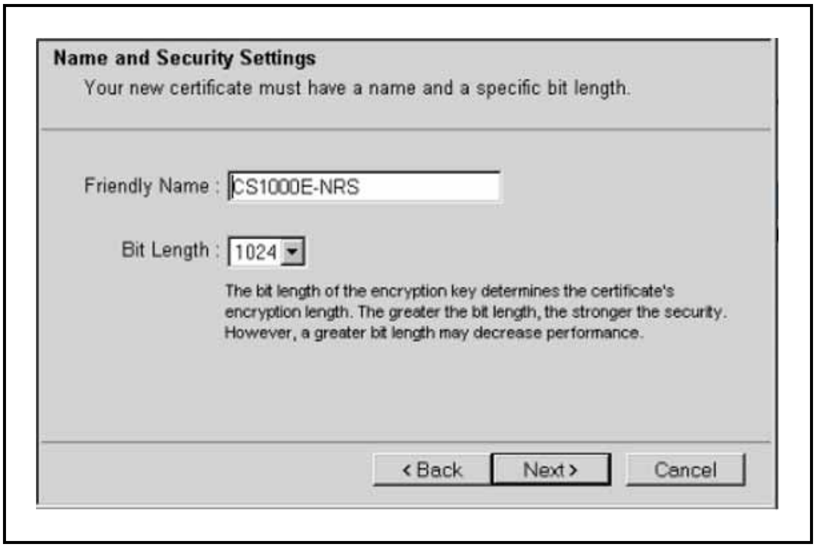
cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

- ● Create a new certificate, signed by local private Certificate Authority
- ○ Import a certificate and its private key from a file
- ○ Assign an existing certificate
- ○ Create a new self-signed certificate
- ○ Create a new certificate request to be signed by third party Certificate Authority

The **Name and Security Settings** window appears.



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

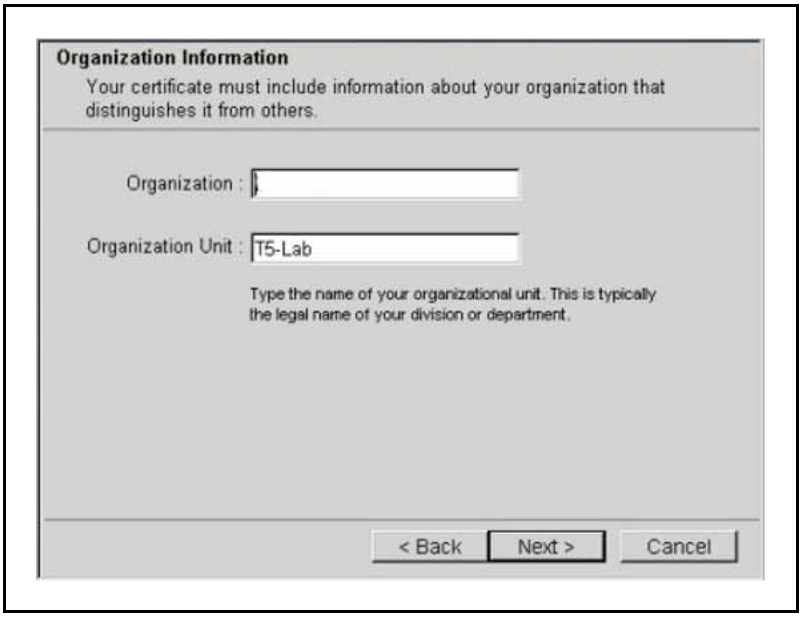
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

5 Type a name in the **Friendly Name** field.

6 Select a bit length from the **Bit length** list.

7 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

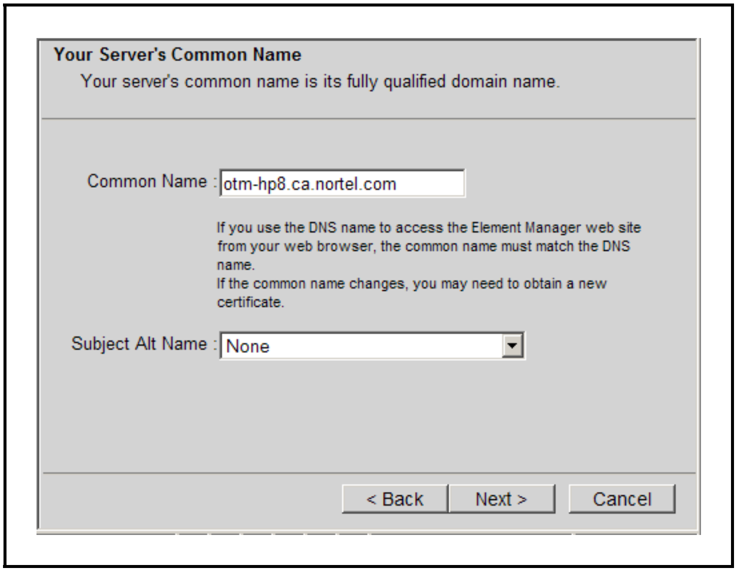
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

8 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

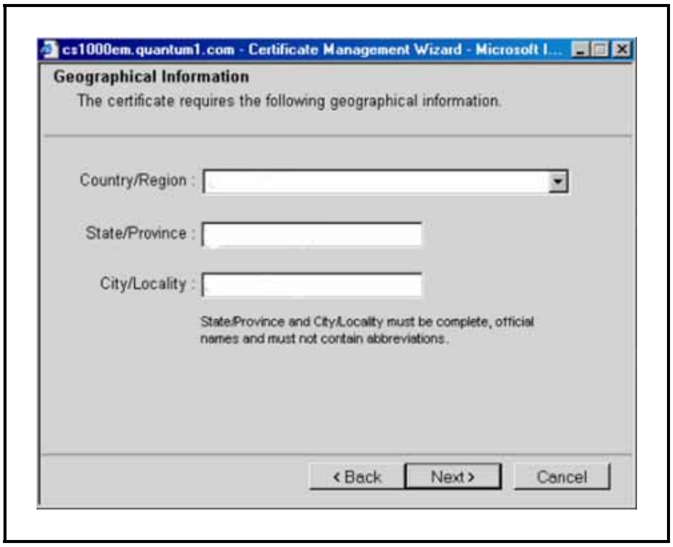
Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name : None

9 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Geographical Information

The certificate requires the following geographical information.

Country/Region :

State/Province :

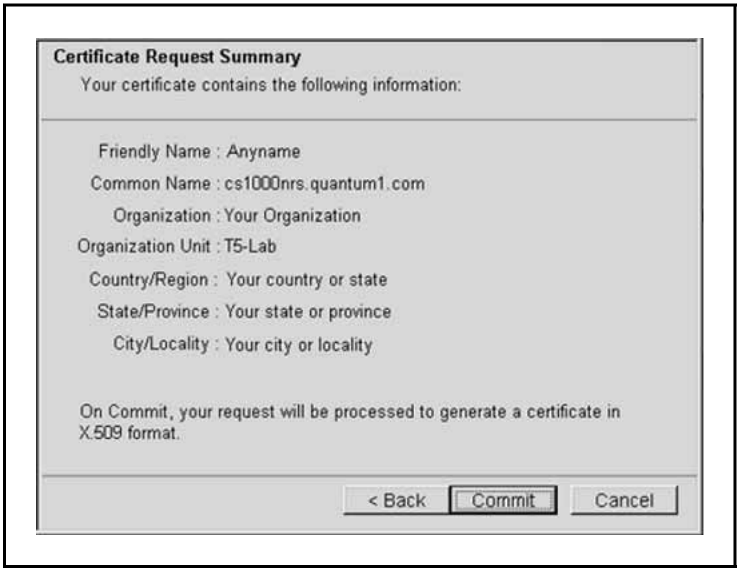
City/Locality :

State/Province and City/Locality must be complete, official names and must not contain abbreviations.

10 In the **Geographical Information** window, perform the following tasks:

- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



Certificate Request Summary

Your certificate contains the following information:

Friendly Name : Anyname

Common Name : cs1000nrs.quantum1.com

Organization : Your Organization

Organization Unit : T5-Lab

Country/Region : Your country or state

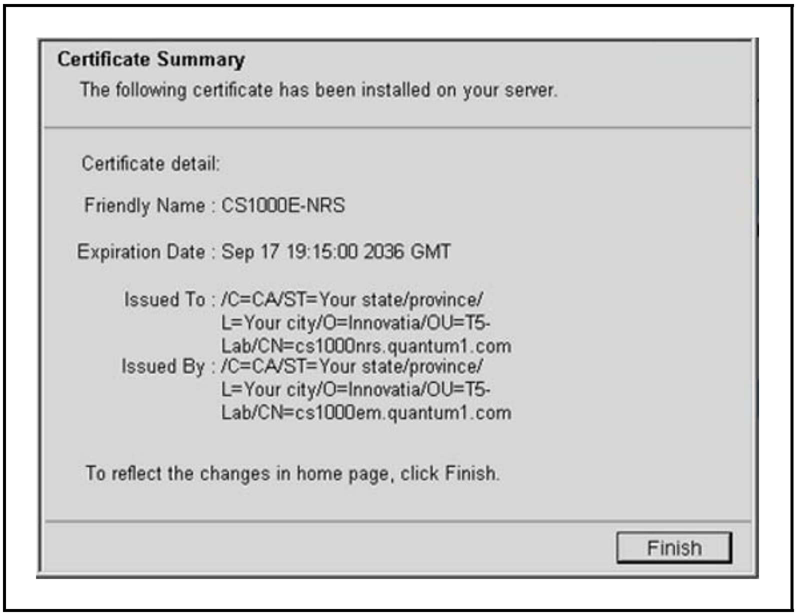
State/Province : Your state or province

City/Locality : Your city or locality

On Commit, your request will be processed to generate a certificate in X.509 format.

11 Click **Commit** to generate a certificate in X.509 format.

A **Certificate Summary** window appears with the certificate information.



Certificate Summary
The following certificate has been installed on your server.

Certificate detail:

Friendly Name : CS1000E-NRS

Expiration Date : Sep 17 19:15:00 2036 GMT

Issued To : /C=CA/ST=Your state/province/L=Your city/O=Innovatia/OU=T5-Lab/CN=cs1000nrs.quantum1.com
Issued By : /C=CA/ST=Your state/province/L=Your city/O=Innovatia/OU=T5-Lab/CN=cs1000em.quantum1.com

To reflect the changes in home page, click Finish.

12 Click **Finish**.

The status changes to signed.

13 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Create a certificate for SIP TLS signed by a public CA

Use the procedures in this section to create a certificate signed by a trusted third-party CA.

If you are upgrading a SIP Gateway system from Communication Server 1000 Release 4.5 or later to Communication Server 1000 Release 6.0, see “Create a request for a third-party CA certificate for SIP TLS when upgrading the system” (page 133) before you proceed.

Use the following procedure to create a certificate request to be signed by a third-party CA for a SIP Proxy or new SIP Gateway system.

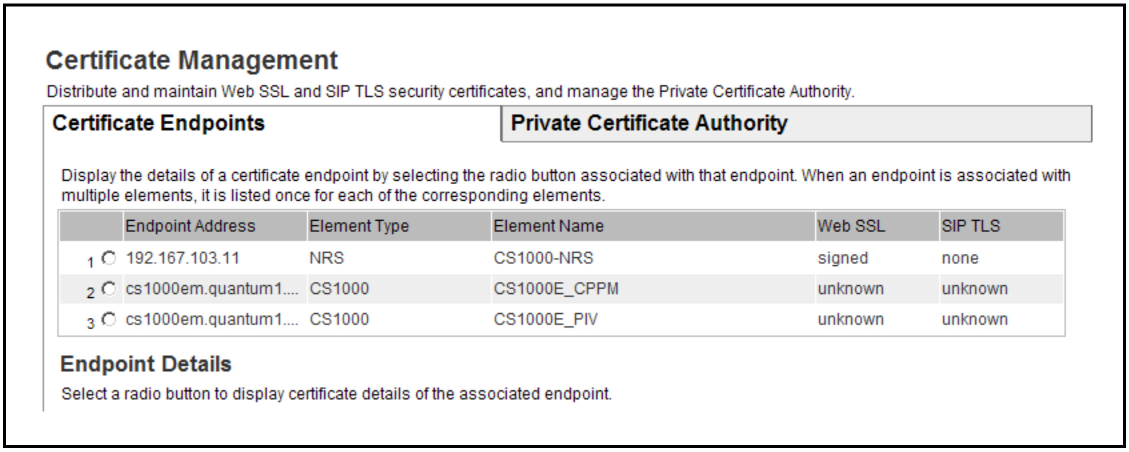
Prerequisites

- Before you create a request for a new certificate signed by a third-party CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 31
Creating a request for a certificate for SIP TLS signed by a public CA

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

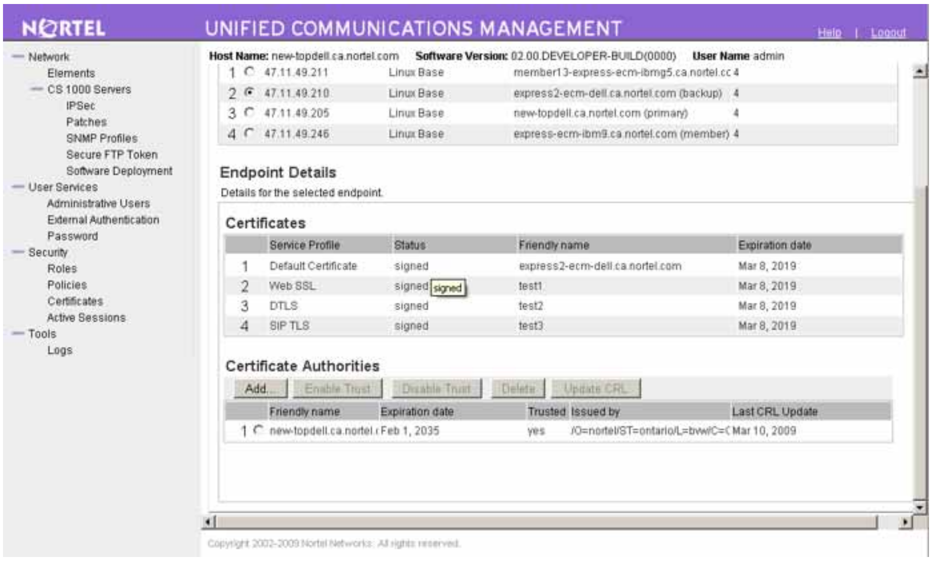
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3	In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

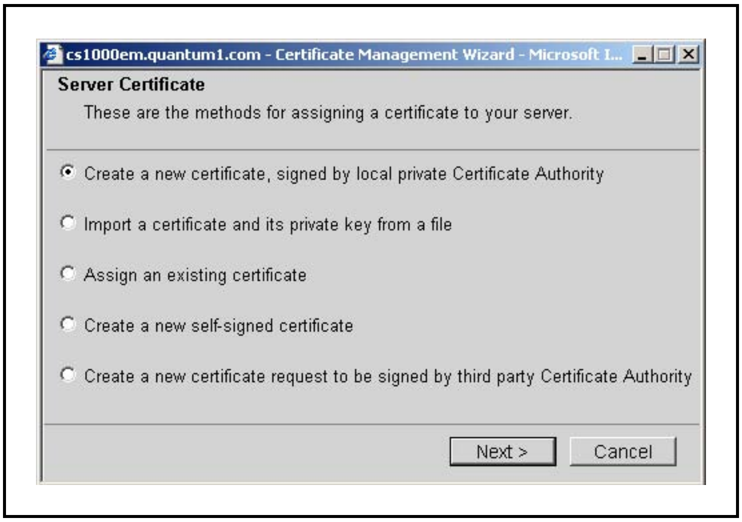
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4	In the Endpoint Details pane, under Certificates, click **SIP TLS**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

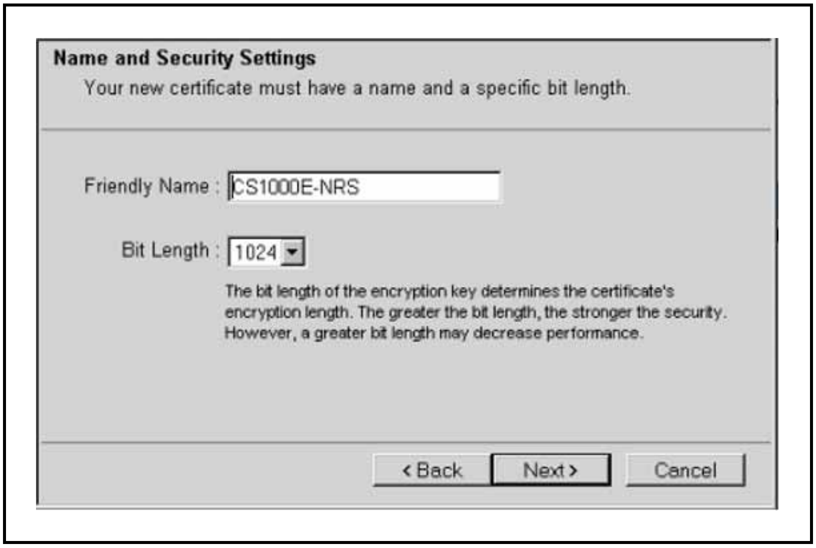
○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Create a new certificate request to be signed by third party** and click **Next**.

The **Name and Security Settings** window appears.


Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

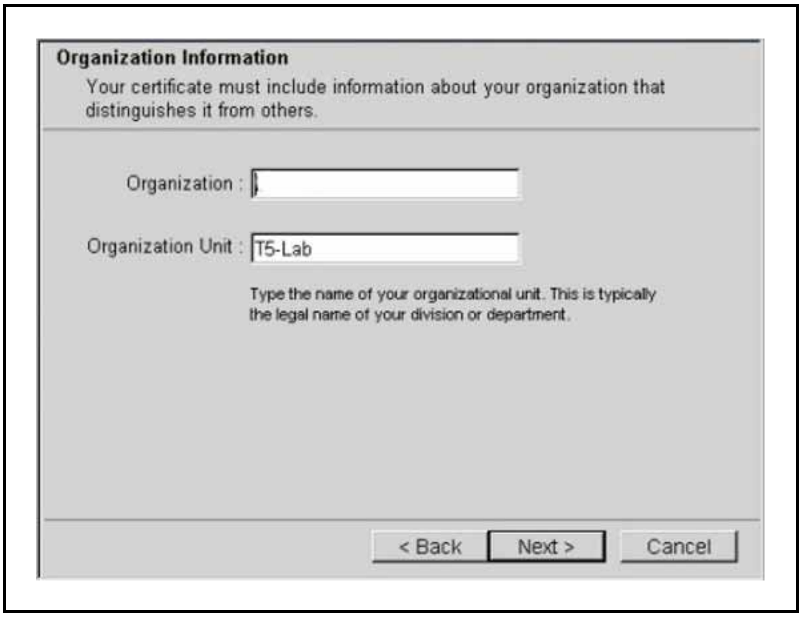
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

6 Type a name in the **Friendly Name** field.

7 Select a bit length from the **Bit length** list.

8 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

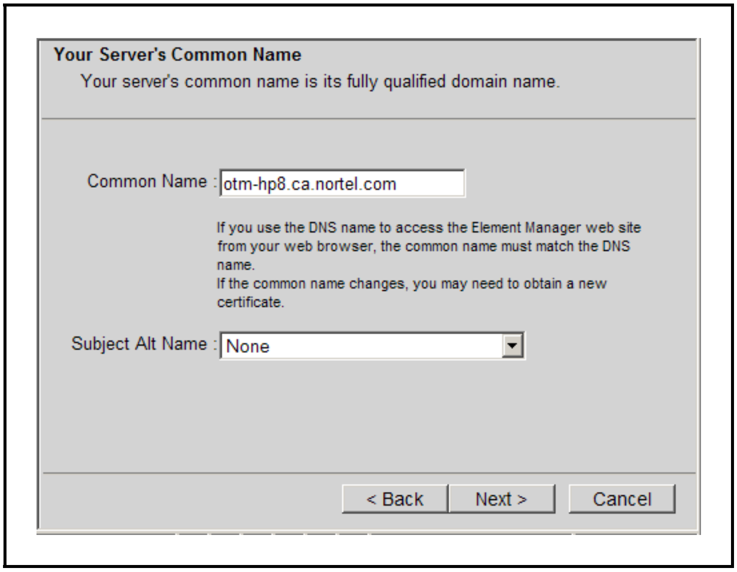
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

9 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name : None

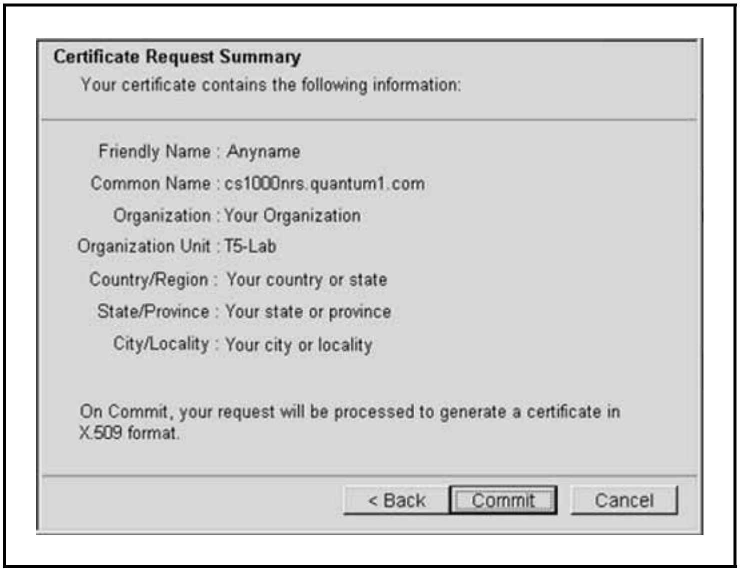
10 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.

11 In the **Geographical Information** window, perform the following tasks:

- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



Certificate Request Summary

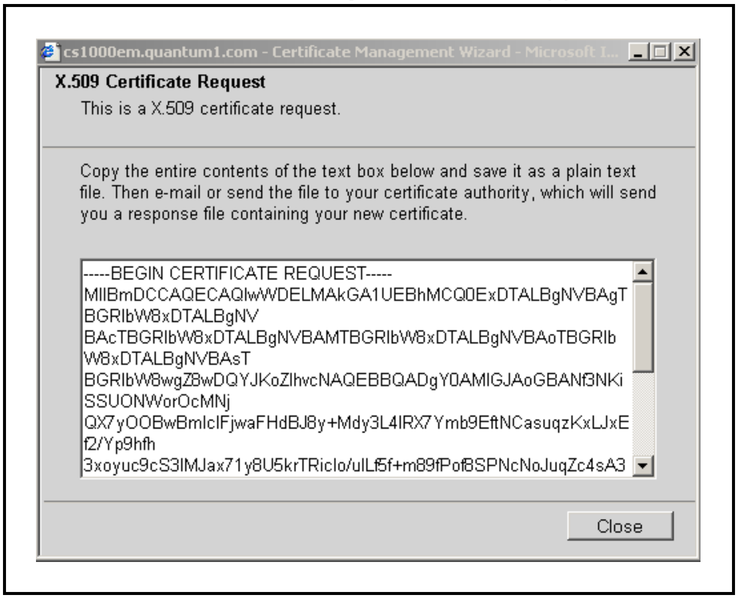
Your certificate contains the following information:

Friendly Name : Anyname
Common Name : cs1000nrs.quantum1.com
Organization : Your Organization
Organization Unit : T5-Lab
Country/Region : Your country or state
State/Province : Your state or province
City/Locality : Your city or locality

On Commit, your request will be processed to generate a certificate in X.509 format.

12 Click **Commit**.

The **X.509 Certificate Request** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

X.509 Certificate Request

This is a X.509 certificate request.

Copy the entire contents of the text box below and save it as a plain text file. Then e-mail or send the file to your certificate authority, which will send you a response file containing your new certificate.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmDCCAQECAQIwWDELMAkGA1UEBhMCQ0ExDTALBgNVBAgT
BGRlbW8xDTALBgNV
BAcTBGRlbW8xDTALBgNVBAMTBGRlbW8xDTALBgNVBAoTBGRlb
W8xDTALBgNVBAsT
BGRlbW8wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANf3NKi
SSUONWorOcMNj
QX7yOOBwBmIcIFjwaFHdBJ8y+Mdy3L4IRX7Ymb9EftNCasuqzKxLJxE
f2/Yp9hfh
3xoyuc9cS3IMJax71y8U5krTRiclo/uILf5f+m89fPof8SPNcNoJuqZc4sA3
```

The X.509 Certificate Request window contains the certificate signing request (CSR).

13 To copy the CSR, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

14 Paste the certificate text into a text editor, and save it in a plain text file.

15 Click **Close**.

The status changes to pending.

16 Send the CSR to the third-party CA.

After you receive the signed certificate from the third-party CA, use the following steps to process and install the certificate, and then add the text from the third-party CA.

17 To process the pending request and install the certificate, follow the steps in Procedure 35 “Processing a pending certificate request by using UCM” (page 144).

The status changes to signed.

18 Follow the instructions from the third-party CA to download the certificates for the intermediate and root CAs.

19 Follow the steps in Procedure 22 “Adding a CA to an endpoint” (page 100) to add the intermediate CA to the server.

For more information about certificate chains, see Table 3 "Examples of certificates in a chain" (page 27).

20 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Create a request for a third-party CA certificate for SIP TLS when upgrading the system

When you upgrade a SIP Gateway System from Communication Server 1000 Release 4.5 or later to Communication Server 1000 Release 6.0, the steps to install third-party CA-signed certificates vary depending on whether you request and install the certificate before upgrading, or after upgrading.

If you generate a certificate request and process the response for a third-party CA certificate after you upgrade the system, the certificate is not available immediately. It can take some time for the third-party CA to respond, and the amount of time can vary. Until the third-party CA signs and returns the CA, SIP TLS cannot function.

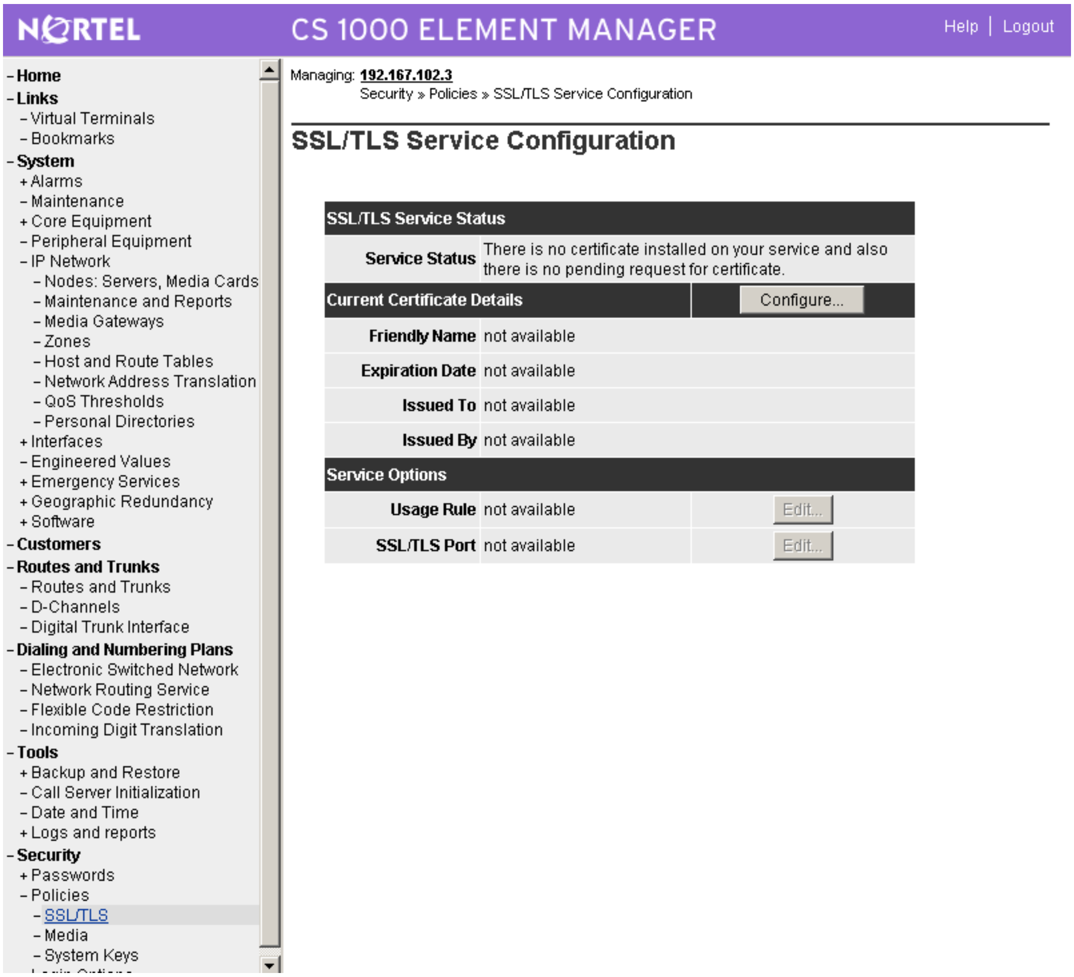
If you have already upgraded the system from Communication Server 1000 Release 4.5 or later to Communication Server 1000 Release 6.0, see Procedure 31 “Creating a request for a certificate for SIP TLS signed by a public CA ” (page 129). If you have not yet upgraded the system see Procedure 32 “Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading” (page 134) before you perform the system upgrade.

Prerequisites

- Before you create a request for a new certificate signed by a third-party CA by using Element Manager, ensure that the certificate endpoint status is:
  There is no certificate installed on your service and also there is no pending request for certificate.

Procedure 32
Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading

Step	Action
1	Before upgrading from CS 1000 Release 5.5, log on to Element Manager using a System password level 2 account.
2	Click **Security > Policies > SSL/TLS**. The **SSL/TLS Service Configuration** page appears.



Managing: 192.167.102.3
Security » Policies » SSL/TLS Service Configuration

SSL/TLS Service Configuration

SSL/TLS Service Status		
Service Status	There is no certificate installed on your service and also there is no pending request for certificate.	
Current Certificate Details		Configure...
Friendly Name	not available	
Expiration Date	not available	
Issued To	not available	
Issued By	not available	
Service Options		
Usage Rule	not available	Edit...
SSL/TLS Port	not available	Edit...

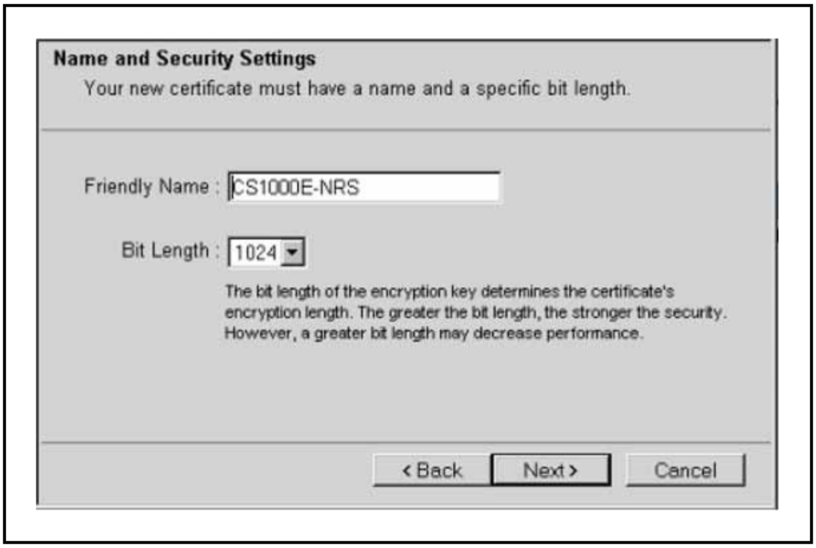
3 Click **Configure**.

The **Server Certificate** window appears.

4 Select **Create a new certificate request to be signed by Certificate Authority**.

5 Click **Next**.

The **Name and Security Settings** window appears.



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

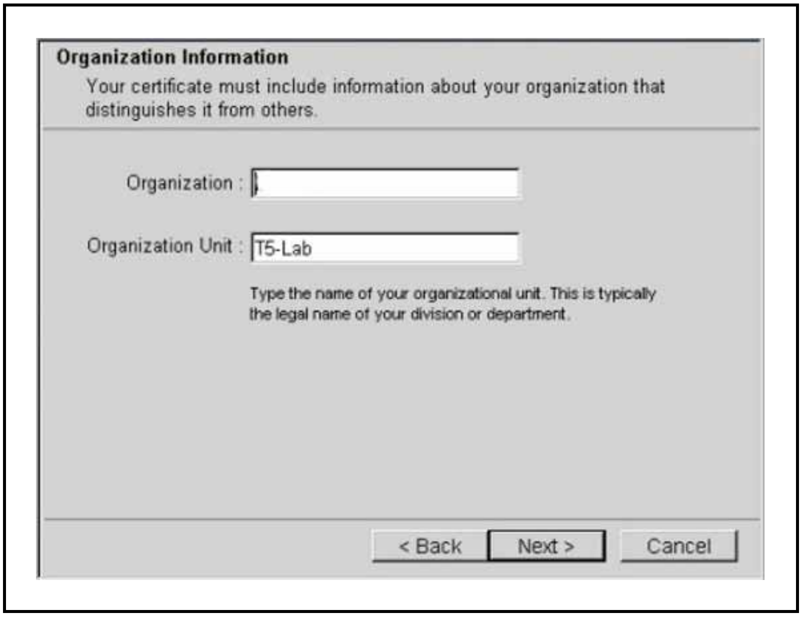
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

6 Type a name in the **Friendly Name** field.

7 Select a bit length from the **Bit length** list.

8 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

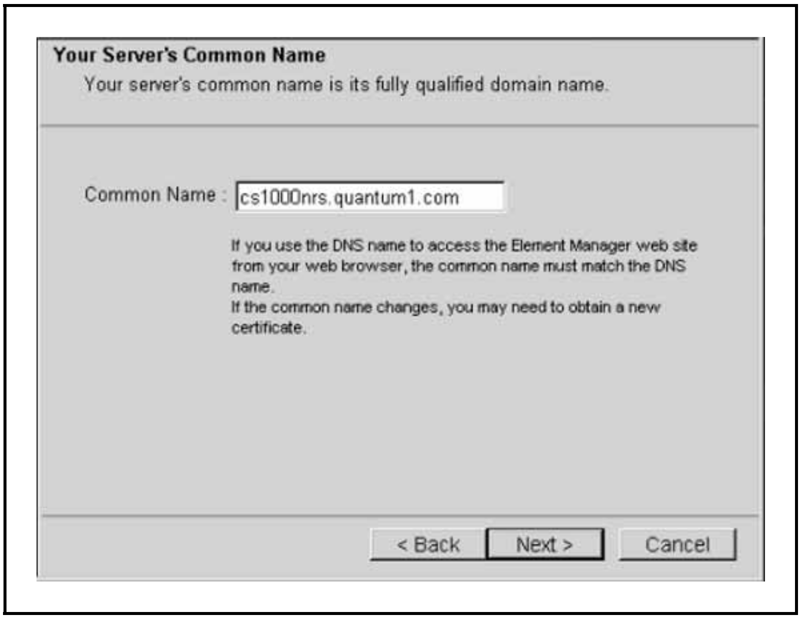
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

9 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

Common Name : cs1000nrs.quantum1.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

10 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

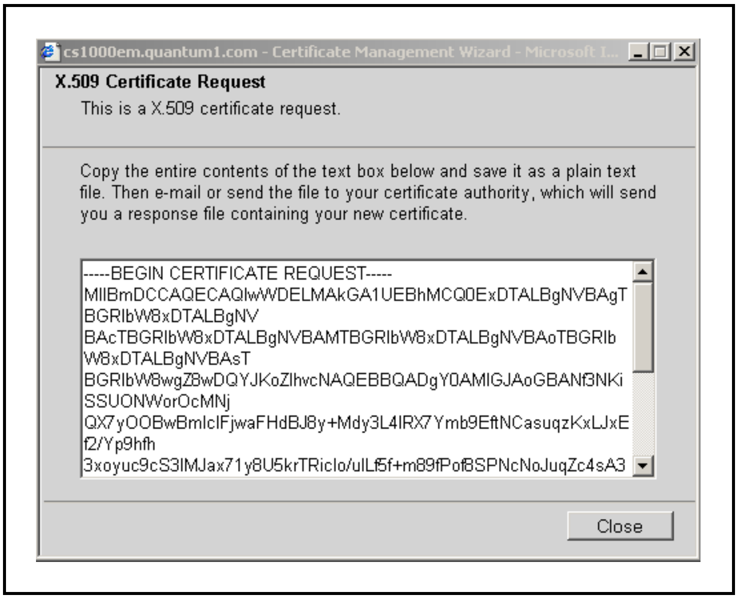
The **Geographical Information** window appears.

11 Perform the following tasks:

- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.

12 The **X.509 Certificate Request** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

X.509 Certificate Request

This is a X.509 certificate request.

Copy the entire contents of the text box below and save it as a plain text file. Then e-mail or send the file to your certificate authority, which will send you a response file containing your new certificate.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmDCCAQECAQIwWDELMAkGA1UEBhMCQ0ExDTALBgNVBAgT
BGRlbW8xDTALBgNV
BAcTBGRlbW8xDTALBgNVBAMTBGRlbW8xDTALBgNVBAoTBGRlb
W8xDTALBgNVBAsT
BGRlbW8wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANf3NKi
SSUONWorOcMNj
QX7yOOBwBmIclFjwaFHdBJ8y+Mdy3L4IRX7Ymb9EftNCasuqzKxLJxE
f2/Yp9hfh
3xoyuc9cS3IMJax71y8U5krTRiclo/uILf5f+m89fPof8SPNcNoJuqZc4sA3
```

The X.509 Certificate Request window contains the certificate signing request (CSR).

13 To copy the CSR, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

14 Paste the certificate text into a text editor, and save it in a plain text file.

15 Click **Close**.

The status changes to:
There is a pending new Certificate request on your service.

16 Send the CSR to the third-party CA.

--End--

Use the following procedure to process a pending certificate response using Element Manager. If you have already upgraded the system from Communication Server 1000 Release 5.x to Communication Server 1000 Release 6.0, see Procedure 31 “Creating a request for a certificate for SIP TLS signed by a public CA ” (page 129)

- Before you process a pending request using Element Manager, ensure that the certificate endpoint status is:
  There is a pending new Certificate request on your service.

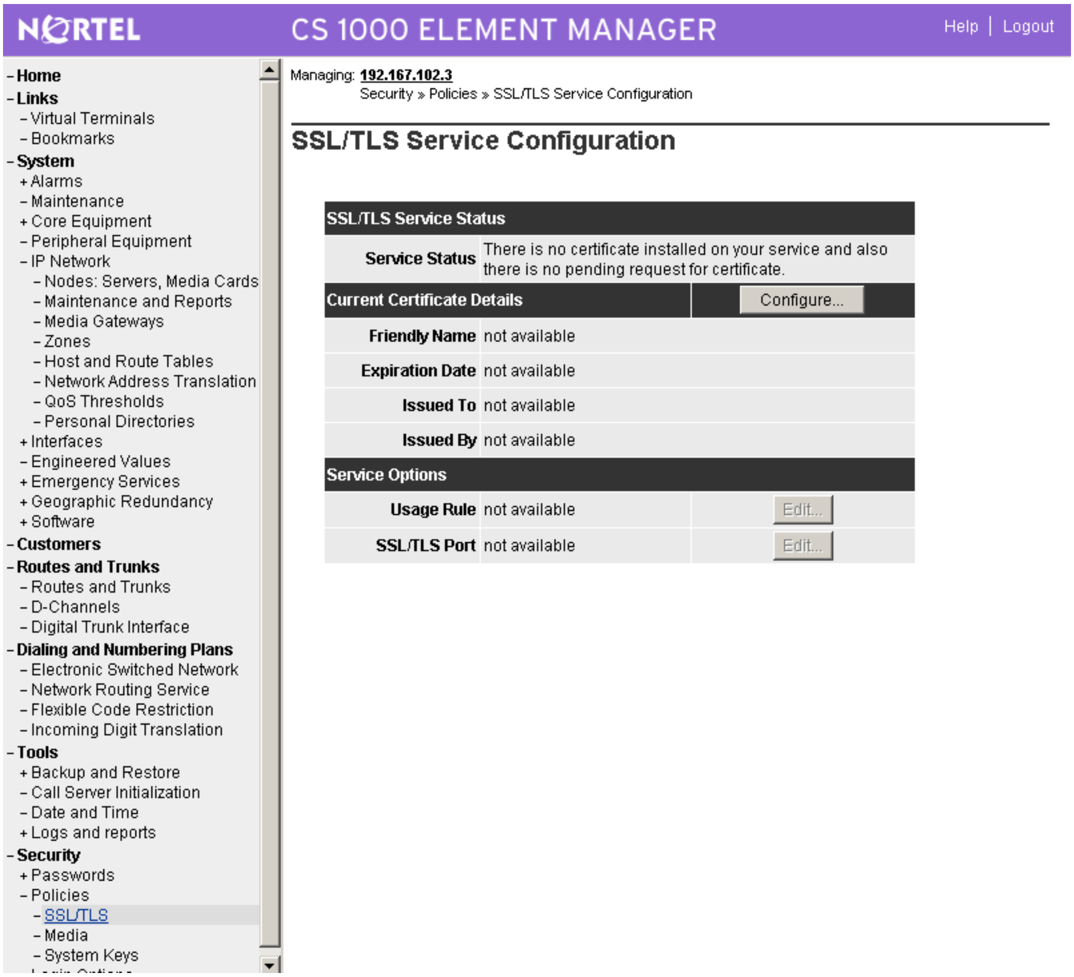
Procedure 33
Processing a pending certificate response for SIP TLS when upgrading

Step Action

1 Before upgrading from CS 1000 Release 5.x, log on to Element Manager using a System password level 2 account.

2 Click **Security > Policies > SSL/TLS**.

The **SSL/TLS Service Configuration** page appears.



Managing: 192.167.102.3
Security » Policies » SSL/TLS Service Configuration

SSL/TLS Service Configuration

SSL/TLS Service Status	
Service Status	There is no certificate installed on your service and also there is no pending request for certificate.
Current Certificate Details	
Friendly Name	not available
Expiration Date	not available
Issued To	not available
Issued By	not available
Service Options	
Usage Rule	not available
SSL/TLS Port	not available

3 Click **Configure**.

The **Server Certificate** window appears.

4 Select **Process the pending request and install the certificate**, and click **Next**.

The **Process a Pending Request** window appears.

5 Copy the contents of the text file received from the CA, and paste them into the text box.

6 Click **Commit**, and then click **Finish**.

7 Upgrade the SIP Gateway system to CS 1000 Release 6.0.

8 Follow the steps in to add an element.

9 Follow the steps in to add an element.

10 Follow the steps in Procedure 41 “Assigning an existing certificate by using UCM” (page 159) to assign the installed third-party CA certificate.

11 Use the steps in Procedure 22 “Adding a CA to an endpoint” (page 100) to add the certificate to the trusted CA list on each of the endpoints that must communicate with the element that owns this certificate.

12 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Create a self-signed certificate for SIP TLS

Use the following procedure to create a new self-signed certificate.

Prerequisites

- Before you create a new self-signed certificate, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

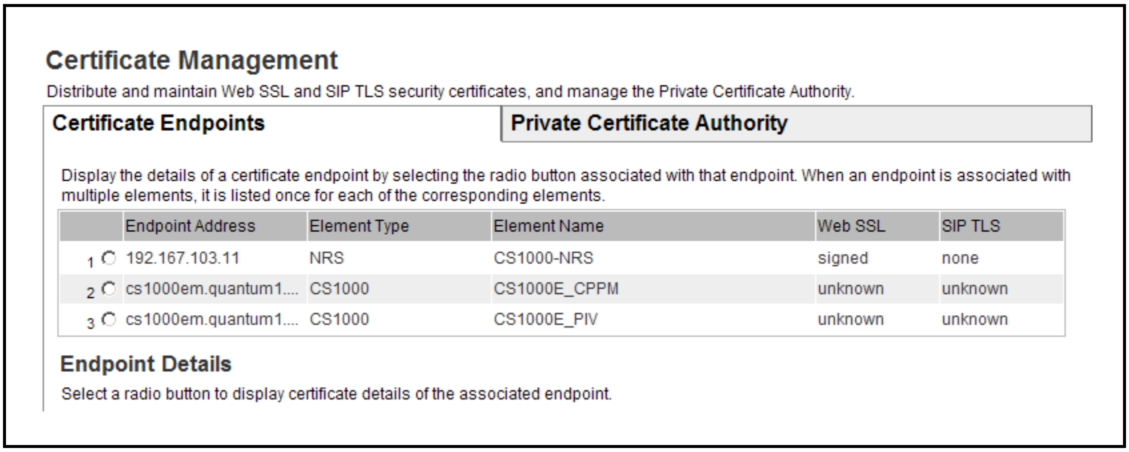
Procedure 34
Creating a self-signed certificate for SIP TLS

Step Action

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

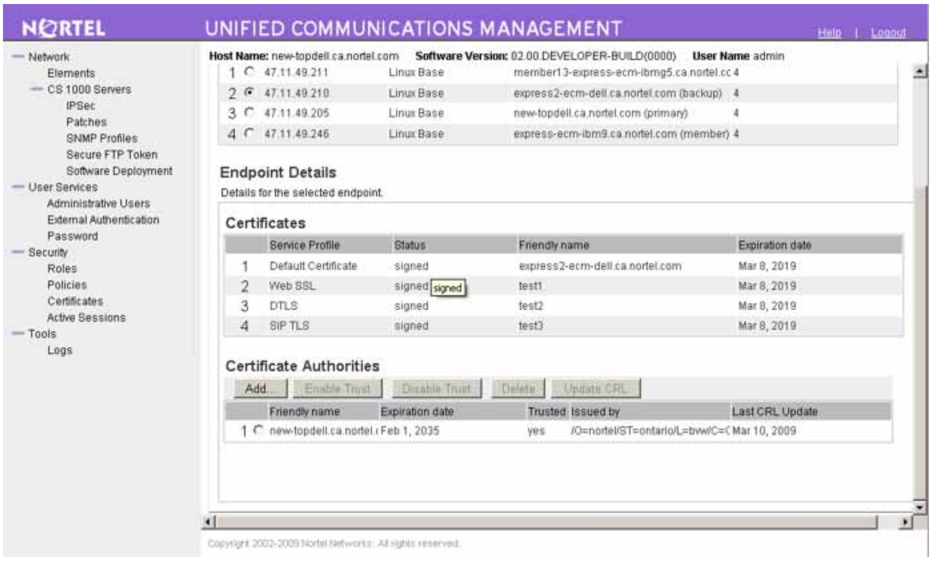
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

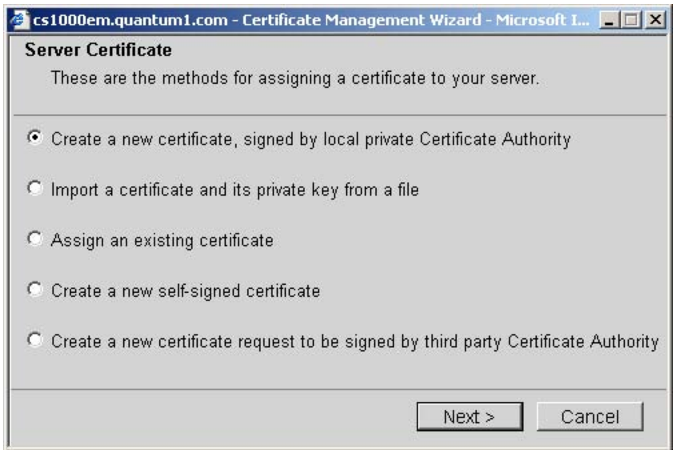
	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.c	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

4 In the Endpoint Details pane, under Certificates, click **SIP TLS**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Next >
Cancel

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

○ Assign an existing certificate

○ Create a new self-signed certificate

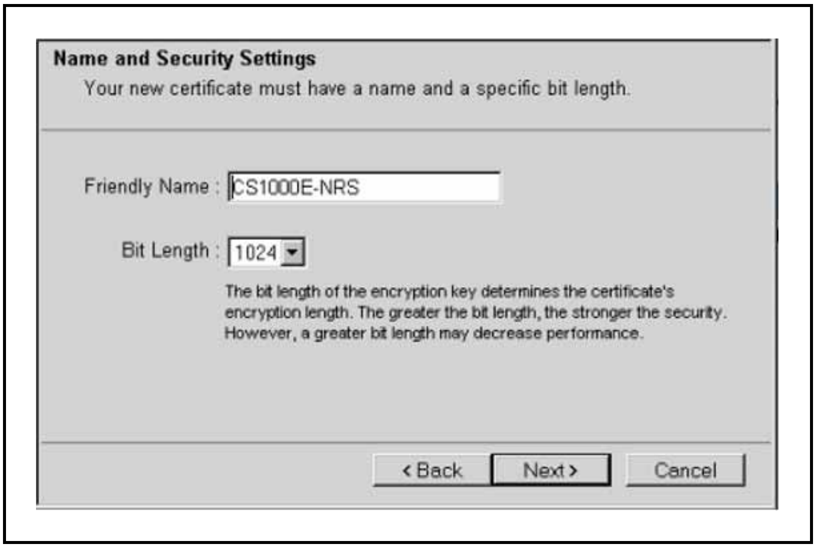
○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Create a new self-signed certificate**, and click **Next**.

The **New Self-Signed Certificate** window appears.

6 Click **Next**.

The **Name and Security Settings** window appears.



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Friendly Name : CS1000E-NRS

Bit Length : 1024

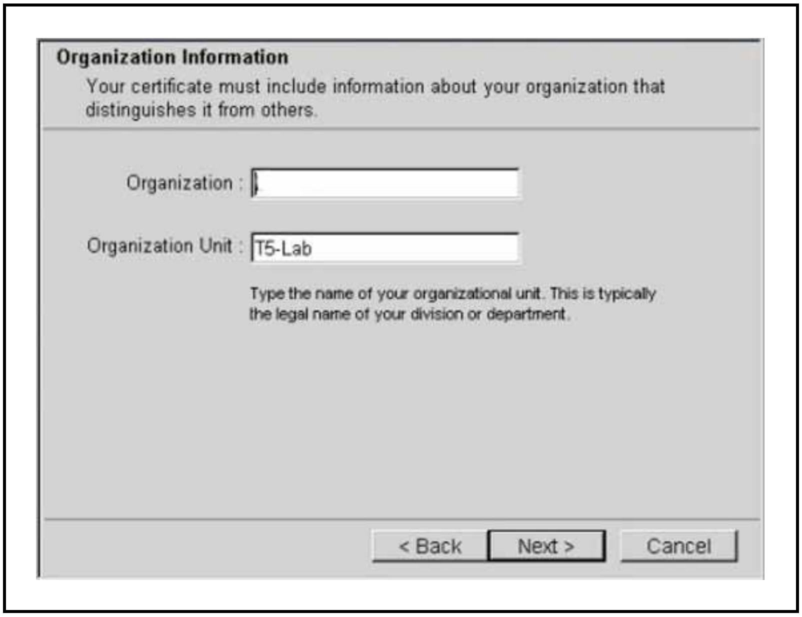
The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

7 Type a name in the **Friendly Name** field.

8 Select a bit length from the **Bit length** list.

9 Click **Next**.

The **Organization Information** window appears.



Organization Information

Your certificate must include information about your organization that distinguishes it from others.

Organization :

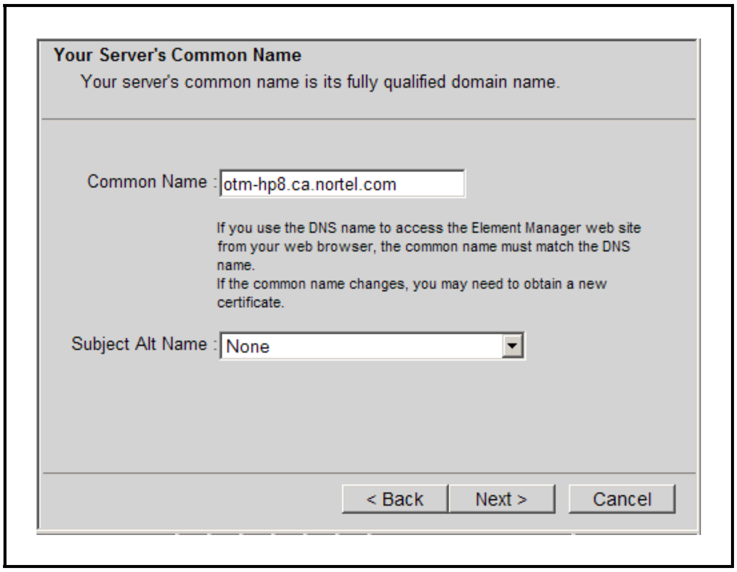
Organization Unit : T5-Lab

Type the name of your organizational unit. This is typically the legal name of your division or department.

10 In the **Organization Information** window, perform the following tasks:

- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

The **Your Server's Common Name** window appears.



Your Server's Common Name

Your server's common name is its fully qualified domain name.

Common Name : otm-hp8.ca.nortel.com

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name : None

11 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.

12 Enter a **Country/Region**.

13 Enter a **State/Province**.

14 Enter a **City/Locality**.

15 Click **Next**.

The **Certificate Request Summary** window appears.

16 Click **Commit**.

The **Certificate Summary** window appears.

17 Click **Finish**.

The status changes to self-signed.

18 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

19 Use the steps in Procedure 38 “Exporting the current self-signed certificate by using UCM” (page 151) to export the self-signed certificate.

20 Use the steps in Procedure 22 “Adding a CA to an endpoint” (page 100) to add the self-signed certificate into the trusted CA list on each of the endpoints that must communicate with the element that owns this certificate.

--End--

Process a pending certificate response

To create a request for a CA to sign a certificate, see "Create a certificate for SIP TLS signed by a public CA " (page 128). After you submit the certificate request file to a CA, the CA sends a response in a text file.

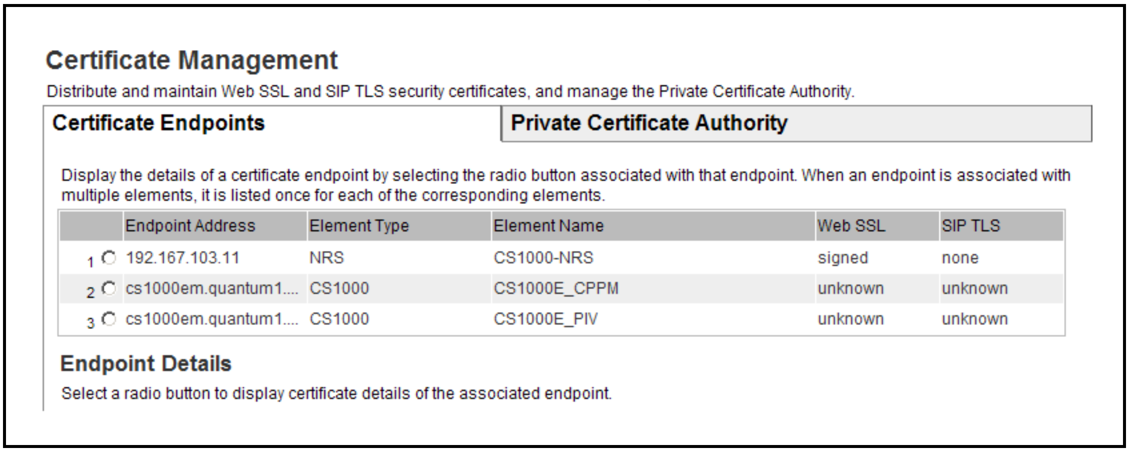
Use the following procedure to process a pending certificate by copying the certificate information from the file you received from the CA.

Prerequisites

- Before you process a pending certificate request, ensure that the certificate endpoint status is pending or pending renew. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 35
Processing a pending certificate request by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints | Private Certificate Authority

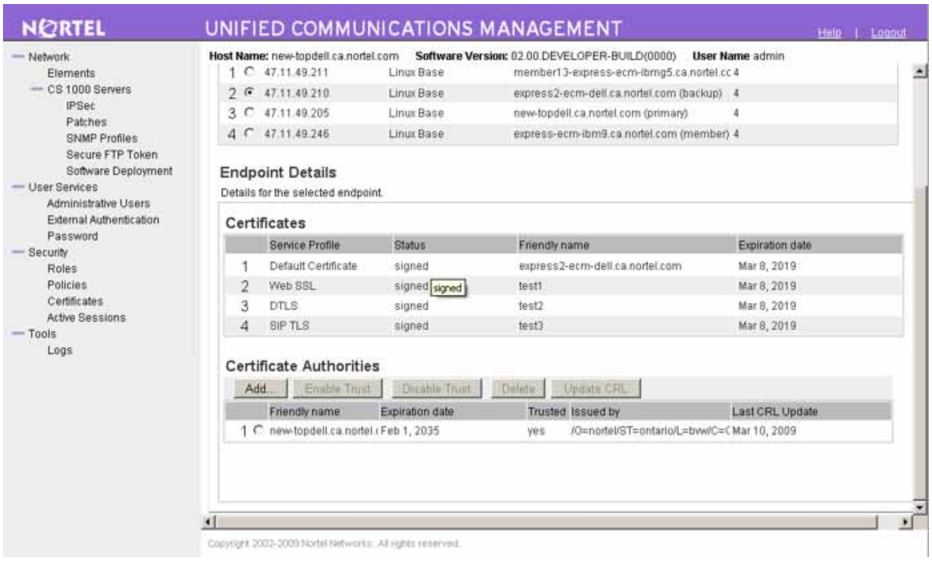
Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

Step	Action
3	In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure. The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

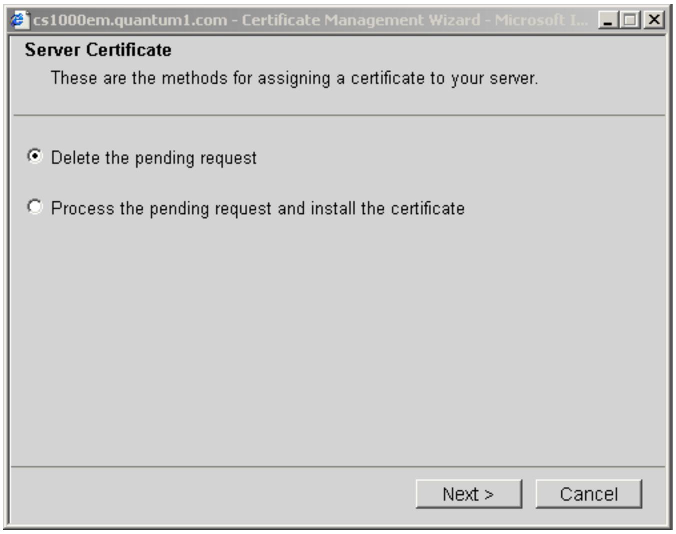
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Next >
Cancel

Server Certificate

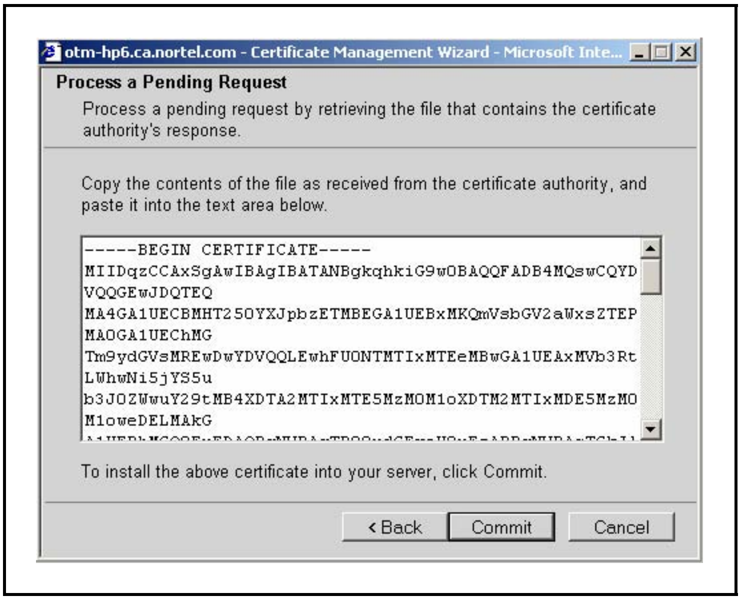
These are the methods for assigning a certificate to your server.

● Delete the pending request

○ Process the pending request and install the certificate

5 Select **Process the pending request and install the certificate**, and click **Next**.

The **Process a Pending Request** window appears.



otm-hp6.ca.nortel.com - Certificate Management Wizard - Microsoft Inte...

Process a Pending Request

Process a pending request by retrieving the file that contains the certificate authority's response.

Copy the contents of the file as received from the certificate authority, and paste it into the text area below.

```
-----BEGIN CERTIFICATE-----
MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQQFADB4MQswCQYD
VQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzETMBEGA1UEBxMKQmVsbGV2aWxsZTEP
MA0GA1UEChMG
Tm9ydGVsMREwDwYDVQQLEwhFU0NTMTIxMTEeMBwGA1UEAxMVb3Rt
LWhwNi5jYS5u
b3J0ZWwuY29tMB4XDTA2MTIxMTE5MzM0M1oXDTM2MTIxMDE5MzM0
M1oweDELMAkG
```

To install the above certificate into your server, click Commit.

6 Copy the contents of the text file you received from the CA and paste it in the text area.

7 Click **Commit**.

The **Certificate Summary** window appears.

8 Click **Finish**.

The service status changes to signed.

--End--

Delete a pending certificate request

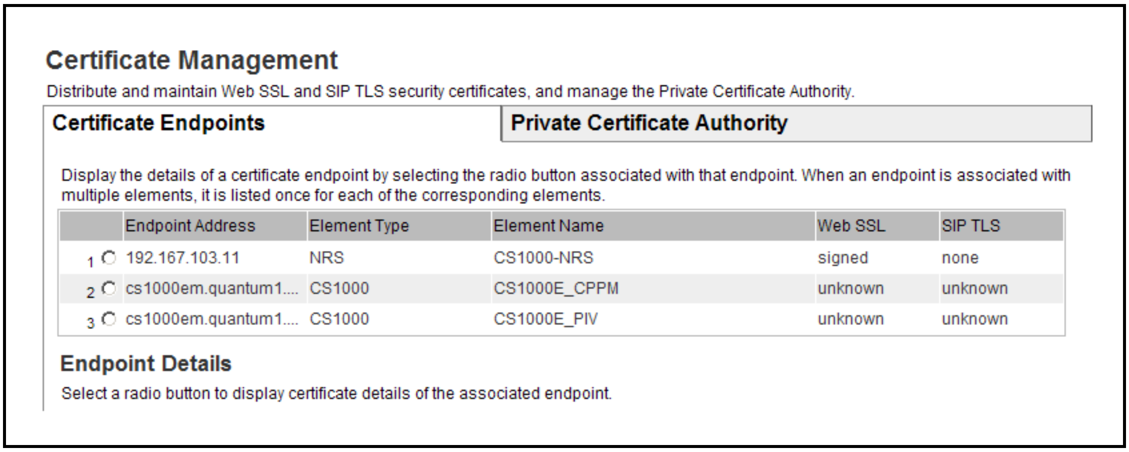
Use the following procedure to delete a pending certificate request.

Prerequisites

- Before you delete a pending certificate request, ensure that the certificate endpoint status is pending. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 36
Deleting a pending certificate request by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

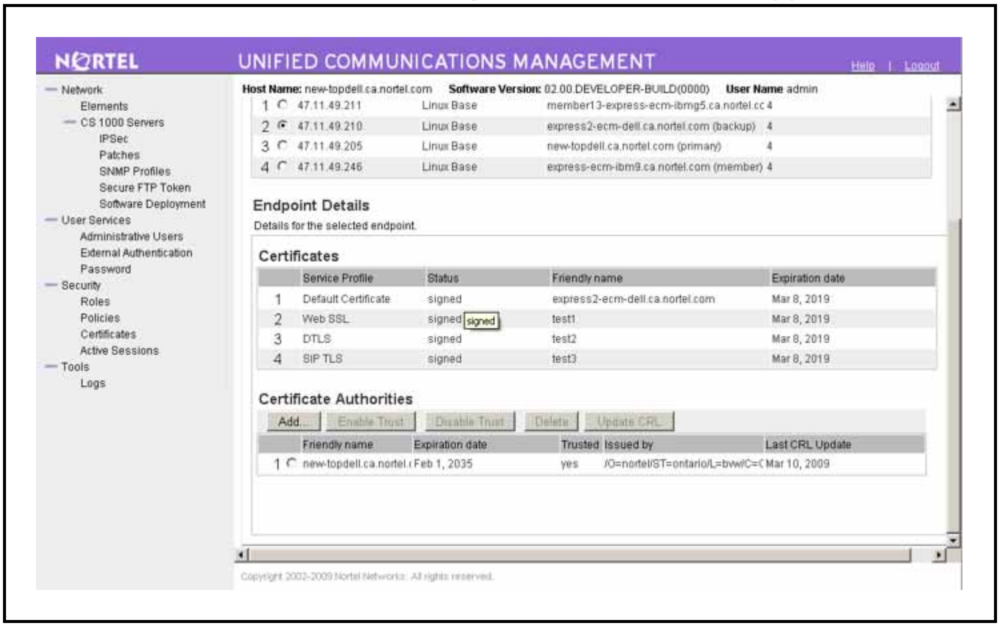
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** pane, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

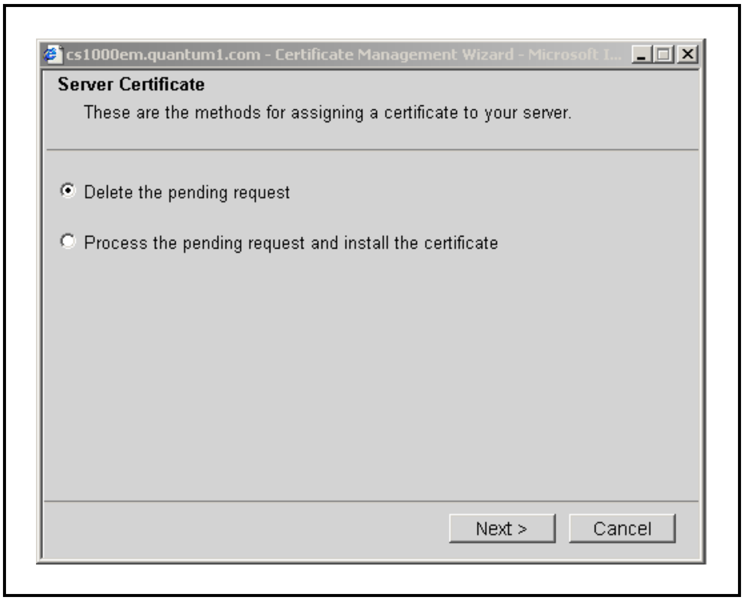
	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.

The **Server Certificate** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Delete the pending request

○ Process the pending request and install the certificate

5 Select **Delete the pending request**, and click **Next**.

The **Delete a Pending Request** window appears.

6 Click **Finish**.

--End--

Create a certificate renew request for the current certificate

The X.509 certificate has an expiration date. A warning message appears if the expiration date is less than 60 days away.

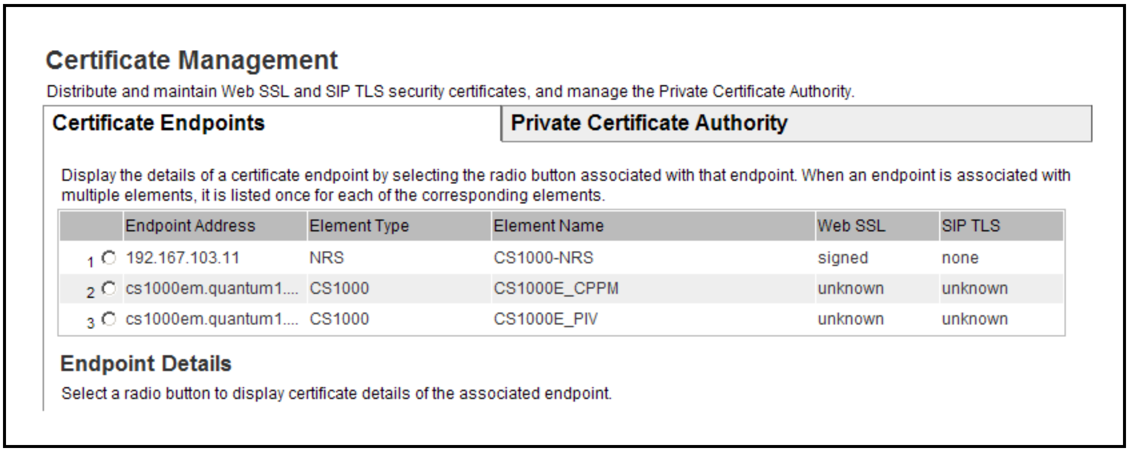
Use the following procedure to create a certificate renewal request.

Prerequisites

- Before you request a certificate renewal, ensure that the certificate endpoint status is signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 37
Creating a certificate renew request by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

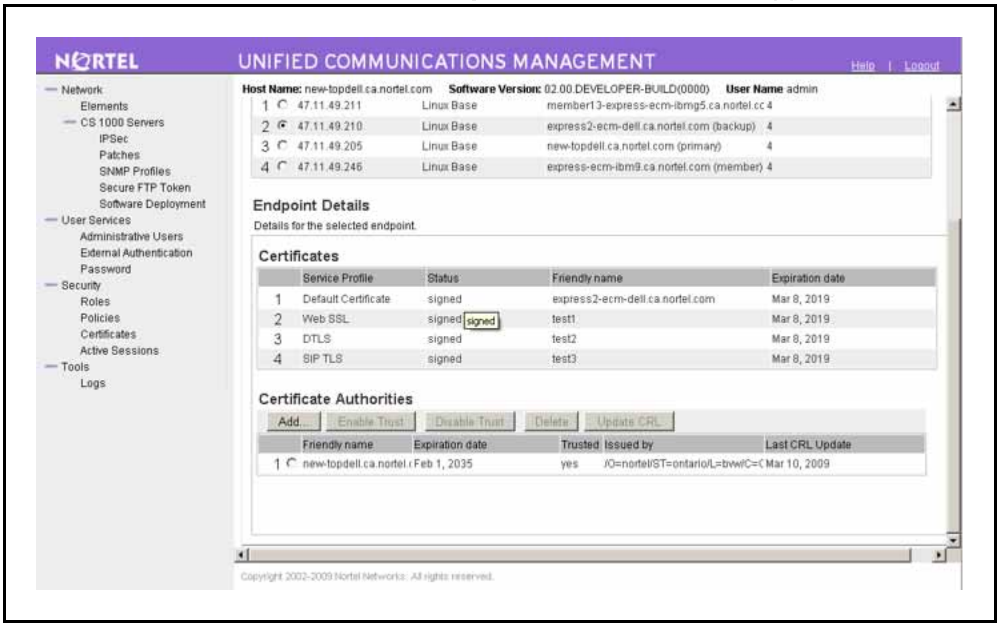
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

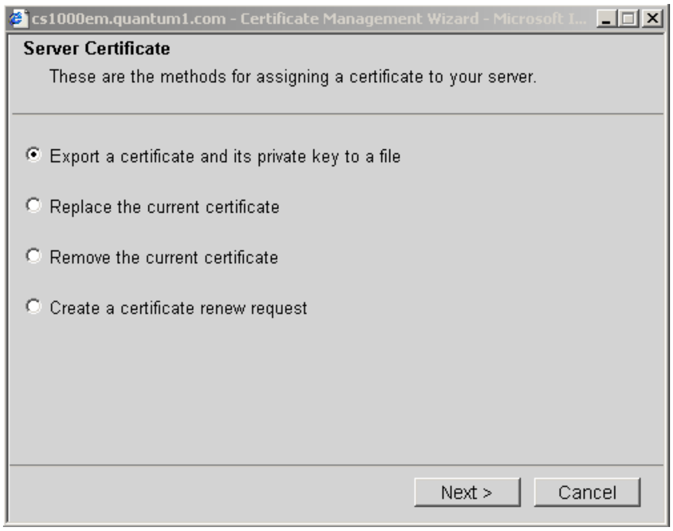
	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Export a certificate and its private key to a file

○ Replace the current certificate

○ Remove the current certificate

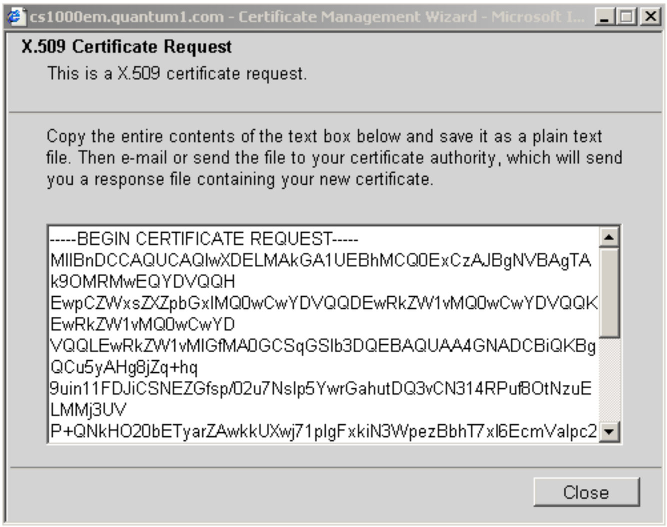
○ Create a certificate renew request

5 Select **Create a certificate renew request**, and click **Next**.

The **Renew Certificate** window appears.

6 Click **Commit** to download the certificate request to a local file.

The **X.509 Certificate Request** window appears. The X.509 Certificate Request window contains the CSR.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

X.509 Certificate Request

This is a X.509 certificate request.

Copy the entire contents of the text box below and save it as a plain text file. Then e-mail or send the file to your certificate authority, which will send you a response file containing your new certificate.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUCAQIwXDELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTA
k9OMRMwEQYDVQQH
EwpCZWxsZXZpbGxlMQ0wCwYDVQQDEwRkZW1vMQ0wCwYDVQQK
EwRkZW1vMQ0wCwYD
VQQLEwRkZW1vMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
QCu5yAHg8jZq+hq
9uin11FDJiCSNEZGfsp/02u7NsIp5YwrGahutDQ3vCN314RPuf8OtNzuE
LMMj3UV
P+QNkHO20bETyarZAwkkUXwj71pIgFxkiN3WpezBbhT7xl6EcmValpc2
```

7 To copy the CSR, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

8 Paste the certificate text into a text editor, and save it in a plain text file.

9 Click **Close**.

--End--

Export the current self-signed certificate

You can export the current self-signed certificate, and later import the certificate to configure a trust relationship between different parties.

Use the following procedure to export the current self-signed certificate.

Prerequisites

- Before you export the current self-signed certificate, ensure that the certificate endpoint status is self-signed. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

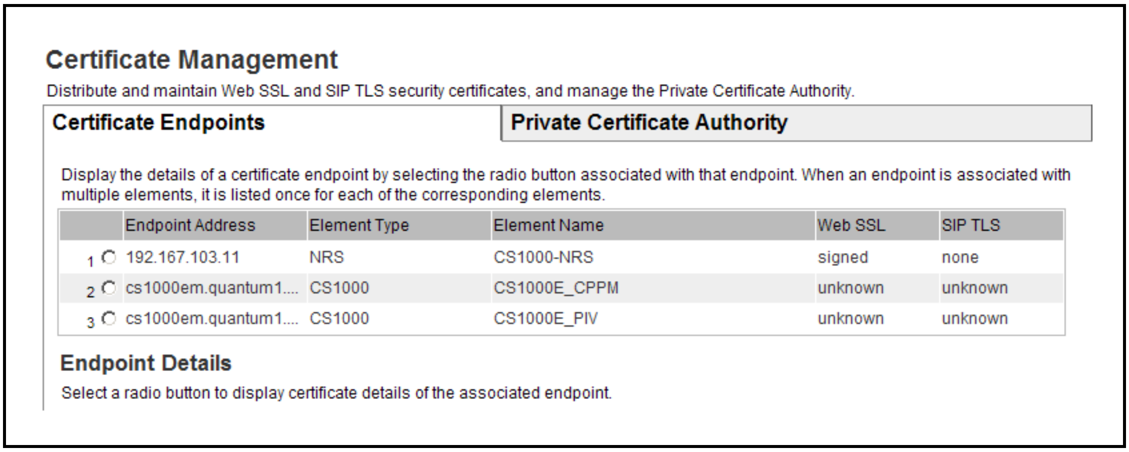
Procedure 38
Exporting the current self-signed certificate by using UCM

Step **Action**

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints | **Private Certificate Authority**

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

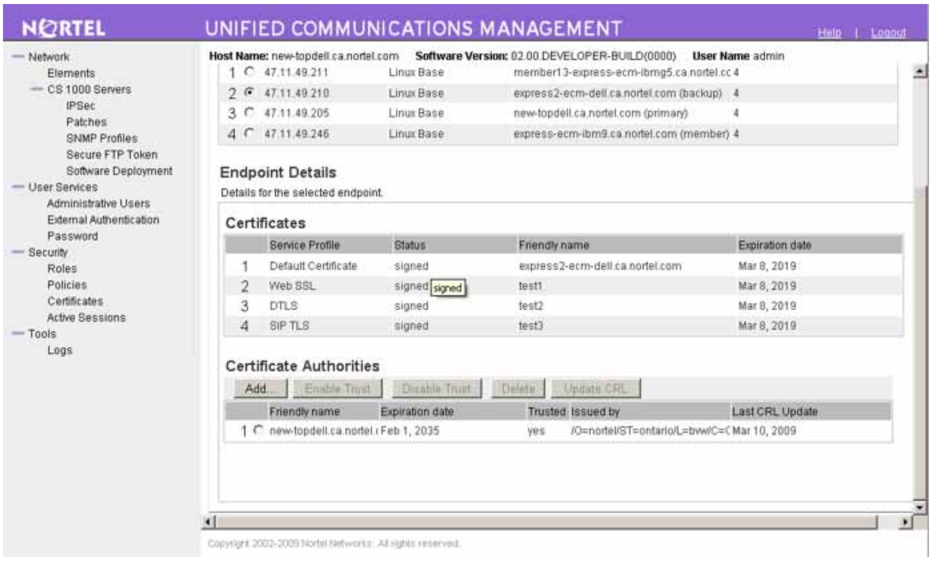
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

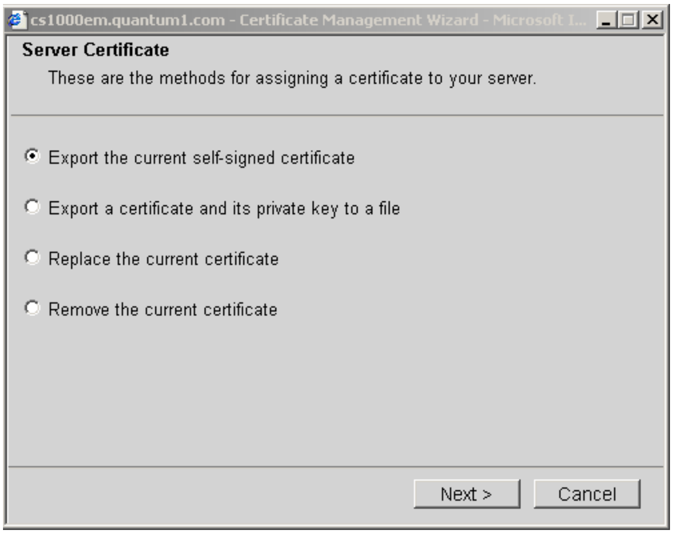
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Next >
Cancel

Server Certificate

These are the methods for assigning a certificate to your server.

● Export the current self-signed certificate

○ Export a certificate and its private key to a file

○ Replace the current certificate

○ Remove the current certificate

5 Select **Export the current self-signed certificate**, and click **Next**.

The **Export Certificate Content** window appears.

6 To copy the certificate information, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

7 Paste the certificate text into a text editor, and save it in a plain text file.

8 Click **Close**.

--End--

Export the current certificate and its private key

You can export the current certificate and its private key into a certificate file. You can use the exported file:

- as a backup copy of the certificate and its private key
- to transfer the certificate and private key to another endpoint.

You must enter a password to encrypt the certificate file, and you must use the same password when you later import the certificate and its key. You can import the certificate and key to another endpoint using the steps in “Import a certificate and its private key from a file” (page 156).

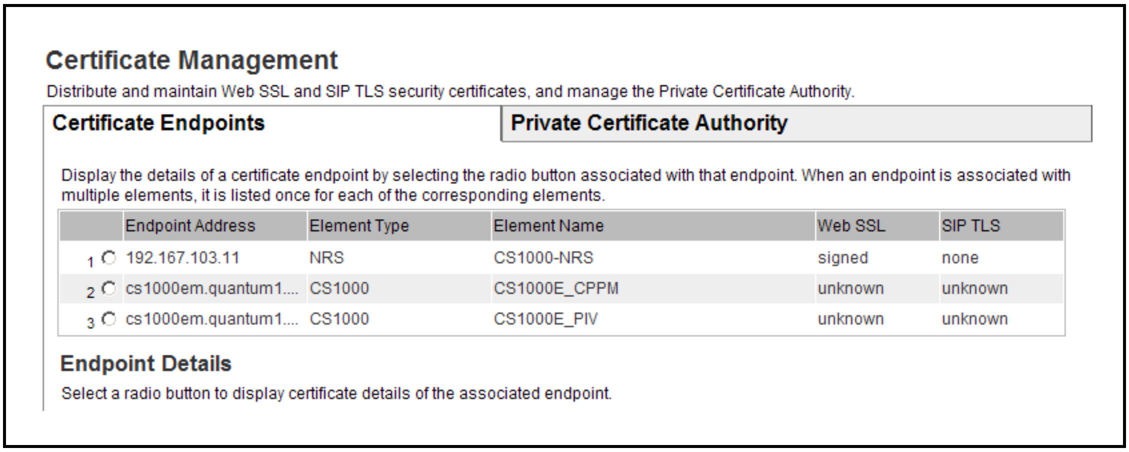
Use the following procedure to export the current certificate and its private key.

Prerequisites

- Before you export the current certificate and its key, ensure that the certificate endpoint status is one of: self-signed, signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 39
Exporting the current certificate and its private key by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

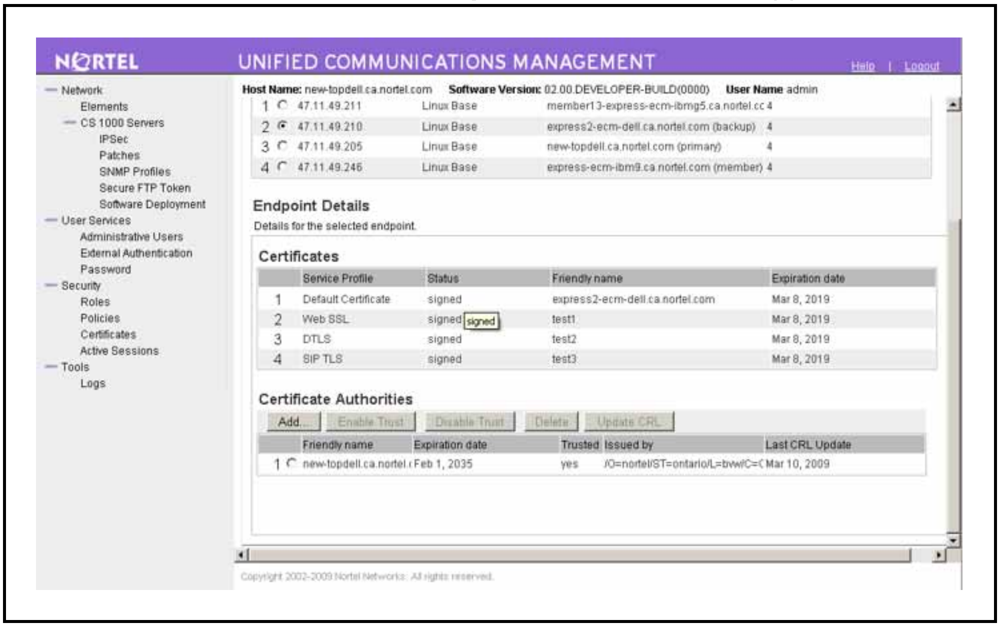
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** tab, select the radio button next to the endpoint from which you want to export the certificate and key.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc 4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup) 4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary) 4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member) 4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

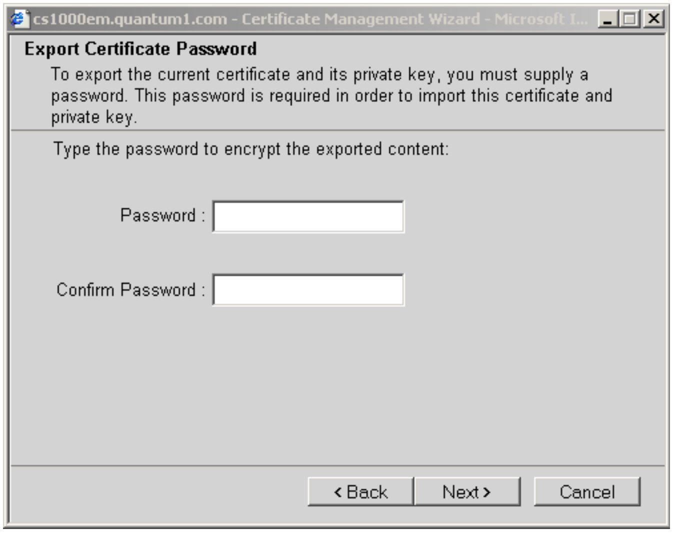
Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.

5 Select **Export a certificate and its private key to a file**, and click **Next**.

The **Export Certificate Password** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
< Back
Next >
Cancel

Export Certificate Password

To export the current certificate and its private key, you must supply a password. This password is required in order to import this certificate and private key.

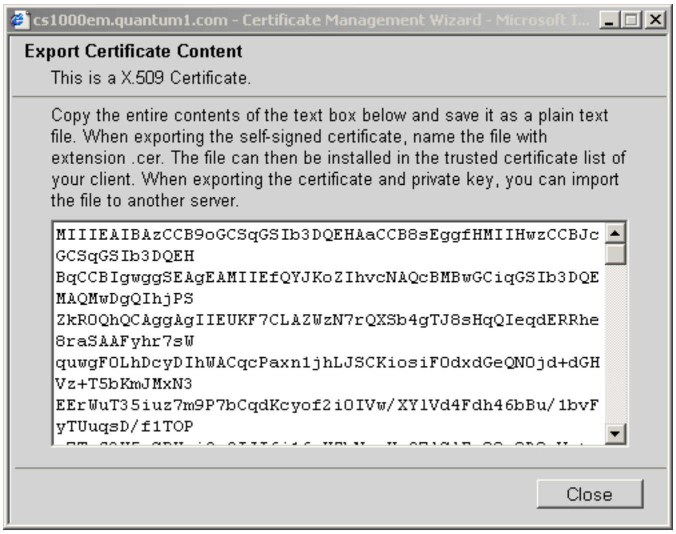
Type the password to encrypt the exported content:

Password :

Confirm Password :

6 Enter the password in the *Password* and *Confirm Password* fields, and click **Next**.

The **Export Certificate Content** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Close

Export Certificate Content

This is a X.509 Certificate.

Copy the entire contents of the text box below and save it as a plain text file. When exporting the self-signed certificate, name the file with extension .cer. The file can then be installed in the trusted certificate list of your client. When exporting the certificate and private key, you can import the file to another server.

```
MIIIEAIBAzCCB9oGCSqGSIb3DQEHAaCCB8sEggfHMIIHwzCCBJc
GCSqGSIb3DQEH
BqCCBIgwggSEAgEAMIIEfQYJKoZIhvcNAQcBMBwGCiqGSIb3DQE
MAQMwDgQIhjPS
ZkROQhQCAggAgIIEUKF7CLAZWzN7rQXSb4gTJ8sHqQIeqdERRhe
8raSAAFyhr7sW
quwgFOLhDcyDIhWACqcPaxn1jhLJSCKiosiFOdxdGeQNOjd+dGH
Vz+T5bKmJMxN3
EErWuT35iuz7m9P7bCqdKcyof2iOIVw/XYlVd4Fdh46bBu/1bvF
yTUuqsD/f1TOP
```

7 To copy the certificate information, click in the text box, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

8 Paste the certificate text into a text editor, and save it in a plain text file.

9 Click **Close**.

--End--

Import a certificate and its private key from a file

You can import a certificate and its private key from another endpoint. Before you do so, you must export the certificate and key using "Export the current certificate and its private key" (page 153). When you import the certificate and key, you must enter the same certificate password that you entered when you exported the certificate and key.

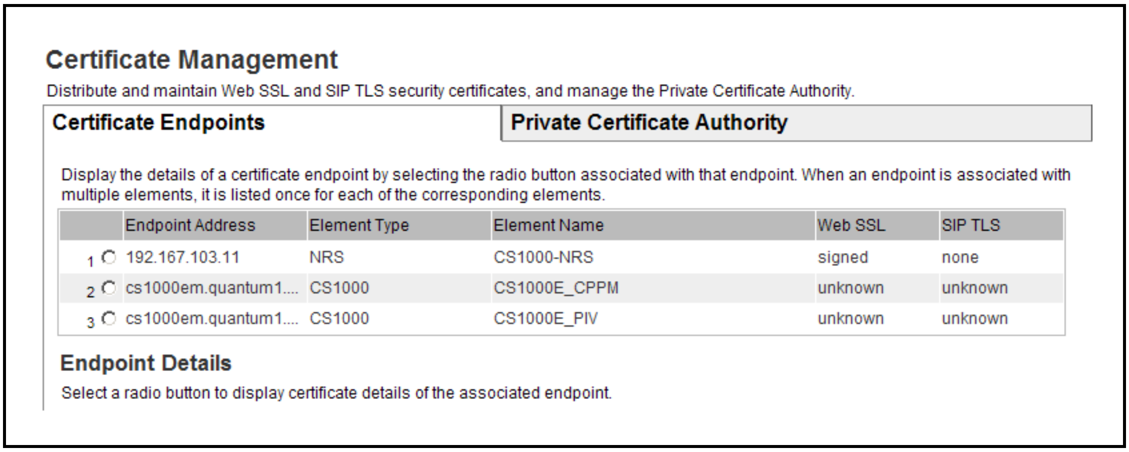
Use the following procedure to import a certificate and its private key to an endpoint.

Prerequisites

- Before you can complete the steps in this procedure, you must export a certificate and its key using the steps in Procedure 39 "Exporting the current certificate and its private key by using UCM" (page 153), and record the password used when you exported the file.
- Before you import a certificate and its key, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 40
Importing a certificate and its private key from a file by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

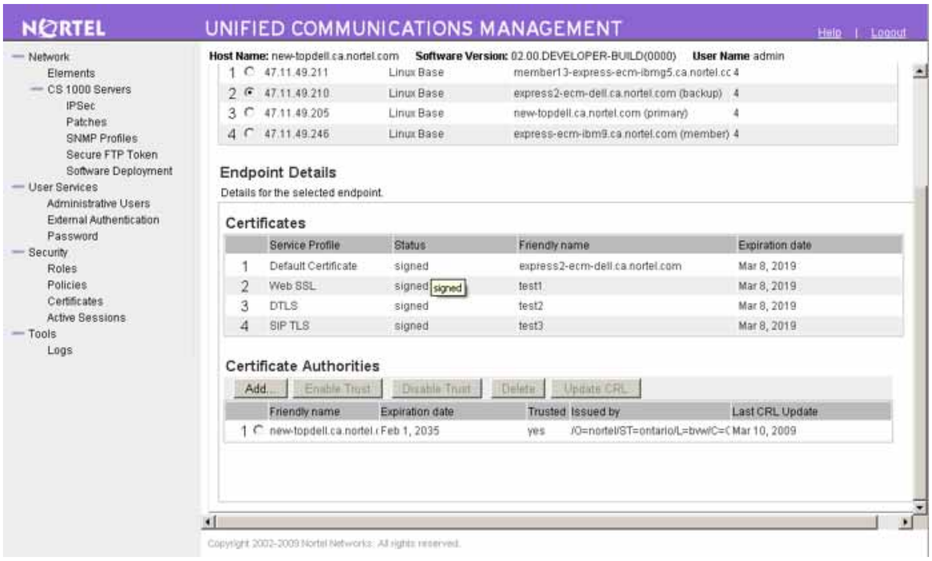
Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

Step	Action
3	In the **Certificate Endpoints** tab, select the radio button next to the endpoint to which you want to import the certificate and key. The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

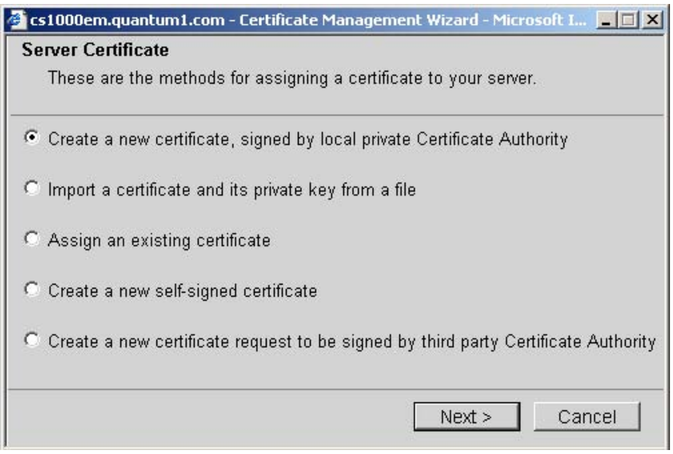
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...
Next >
Cancel

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

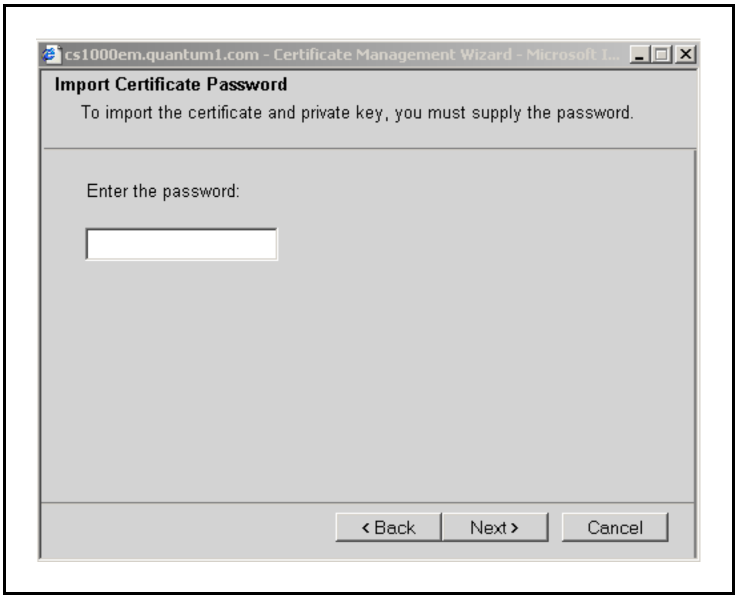
○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Import a certificate and its private key from a file**, and click **Next**.

The **Import Certificate Password** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

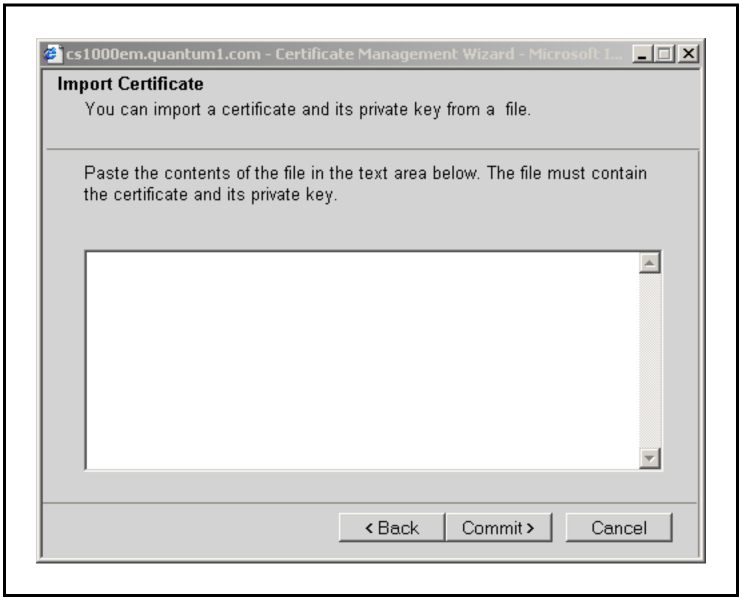
Import Certificate Password

To import the certificate and private key, you must supply the password.

Enter the password:

6 Enter the password of the certificate file, and click **Next**.

The **Import Certificate** window appears.



cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Import Certificate

You can import a certificate and its private key from a file.

Paste the contents of the file in the text area below. The file must contain the certificate and its private key.

7 In the **Import Certificate** window, click in the text box, and press **ctrl-v** to paste the contents of the text file that you exported using the steps in Procedure 39 “Exporting the current certificate and its private key by using UCM” (page 153).

8 Click **Commit**.

The **Certificate Summary** window appears.

9 Click **Finish**.

10 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Assign an existing certificate

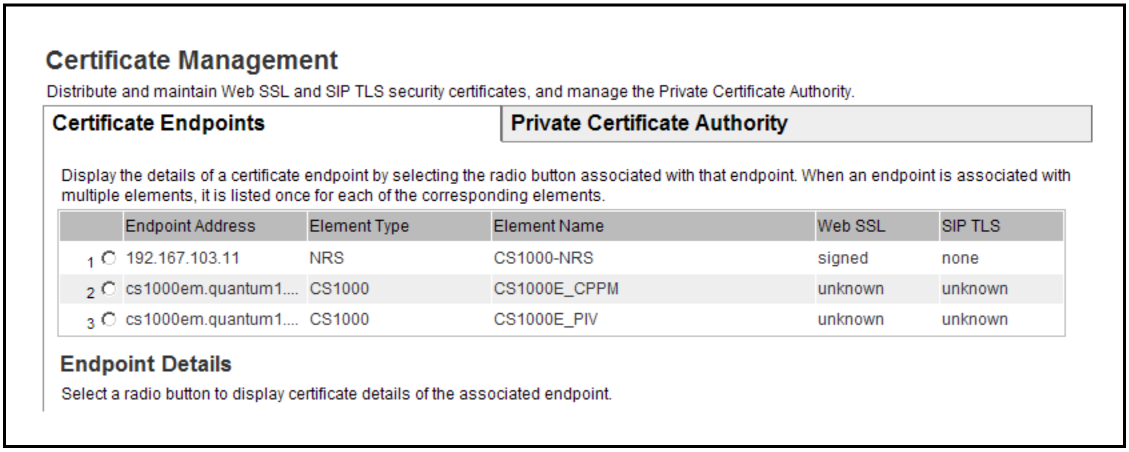
Use the following procedure to assign an existing certificate to an endpoint.

Prerequisites

- Before you assign an existing certificate to an endpoint, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 41
Assigning an existing certificate by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

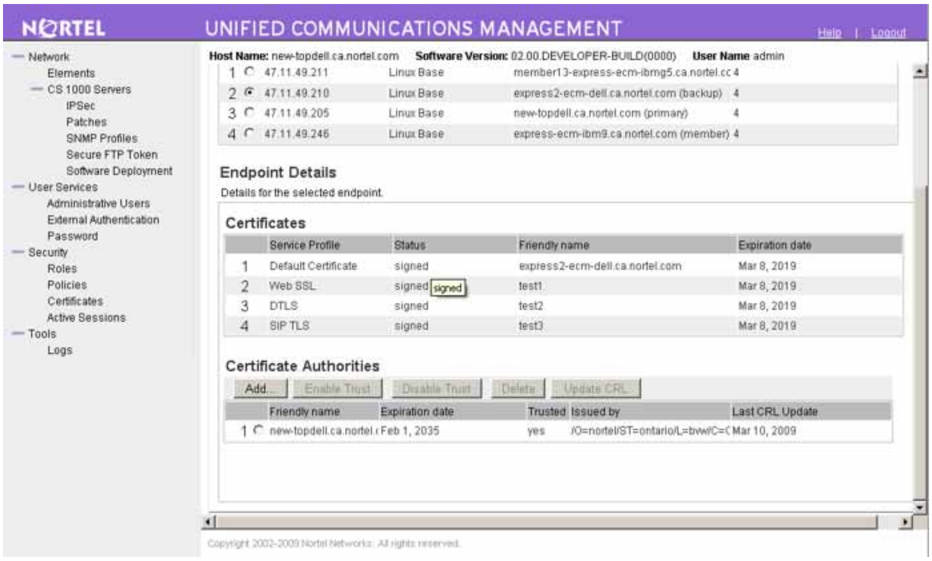
Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

Step	Action
3	In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure. The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1	○ 47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2	● 47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3	○ 47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4	○ 47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

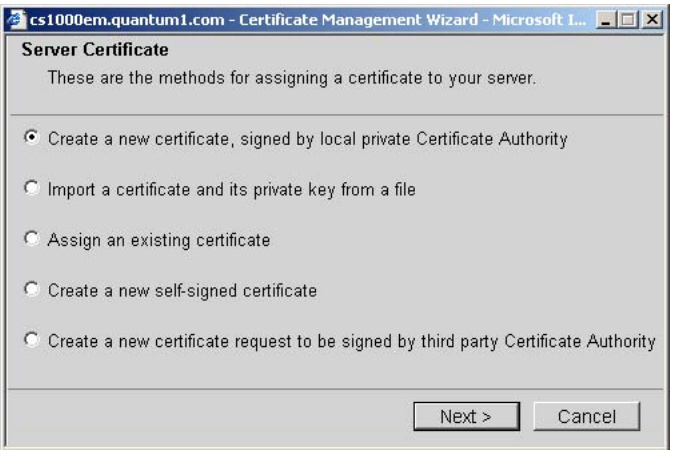
Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.

The **Server Certificate** window appears.


cs1000em.quantum1.com - Certificate Management Wizard - Microsoft I...

Server Certificate

These are the methods for assigning a certificate to your server.

● Create a new certificate, signed by local private Certificate Authority

○ Import a certificate and its private key from a file

○ Assign an existing certificate

○ Create a new self-signed certificate

○ Create a new certificate request to be signed by third party Certificate Authority

5 Select **Assign an existing certificate**, and click **Next**.

The **Available Certificate** window appears.

6 Select a certificate from the list of available certificates, and click **Commit**.

The **Certificate Summary** window appears.

7 Click **Finish**.

8 Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

--End--

Replace the current certificate

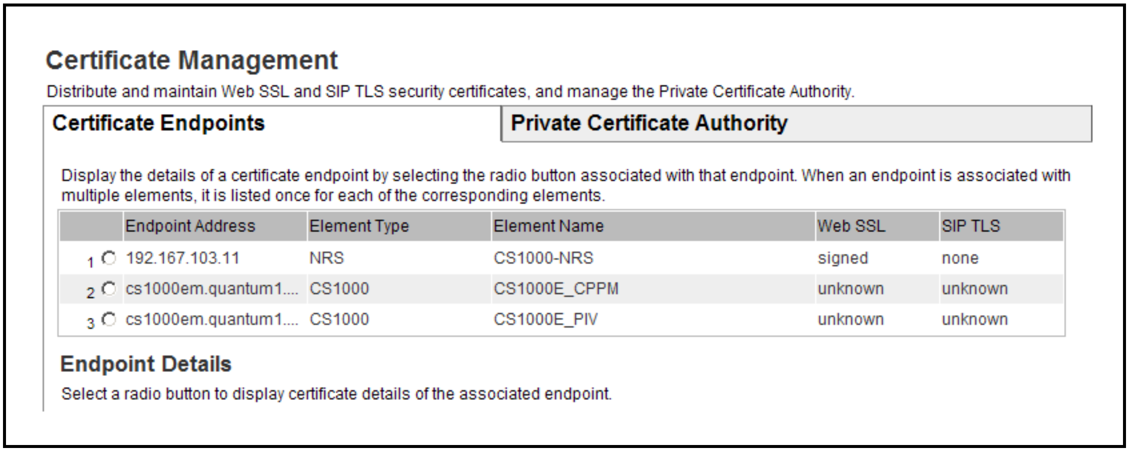
Use the following procedure to replace the current certificate.

Prerequisites

- You can replace a certificate only if more than one certificate is configured.
- Before you replace the current certificate, ensure that the certificate endpoint status is one of: signed, self-signed, expired, or about to expire. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

Procedure 42
Replacing the current certificate by using UCM

Step	Action
1	Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

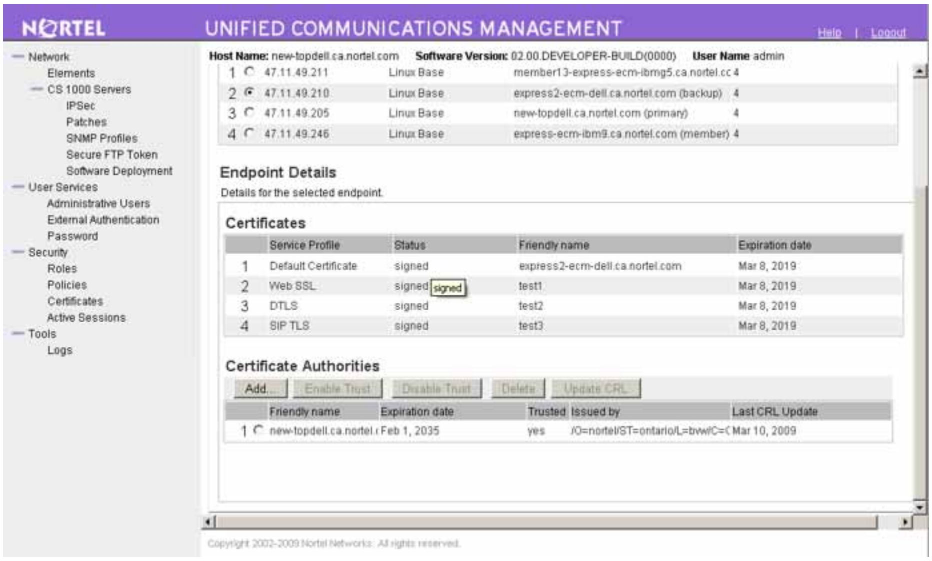
Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

Step	Action
3	In the **Certificate Endpoints** tab, select the radio button next to the endpoint that you want to configure. The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1 ○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2 ●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3 ○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4 ○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

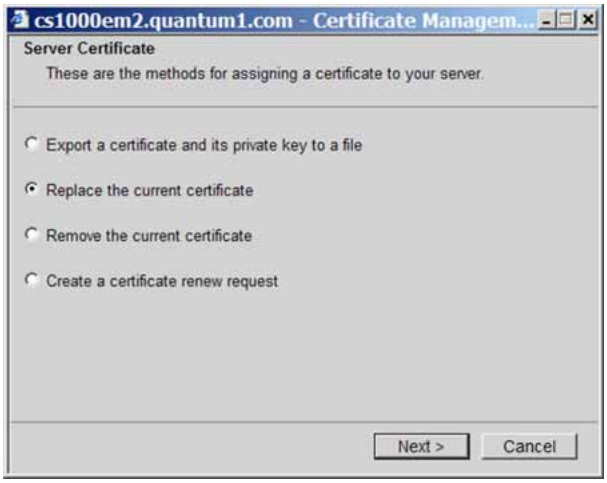
	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.(	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=(	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.

The **Server Certificate** window appears.



Server Certificate

These are the methods for assigning a certificate to your server.

○ Export a certificate and its private key to a file

● Replace the current certificate

○ Remove the current certificate

○ Create a certificate renew request

5 Select **Replace the current certificate**, and click **Next**.

The **Available Certificate** window appears.

6 Select a certificate from the list, and click **Commit**.

The **Certificate Summary** window appears.

7 Click **Finish**.

--End--

Remove the current certificate

Use the following procedure to remove the current certificate.

> **ATTENTION**
> Web SSL and SIP TLS can be disrupted if no certificate is present. Therefore, if you remove the current certificate, you must replace it or install a new one to prevent an interruption of service.

Prerequisites

- Before you remove the current certificate, ensure that the certificate endpoint status is one of: signed, self-signed, expired, or about to expire. For more information about certificate endpoint status types, see Table 24 "Status types for certificate endpoints" (page 104).

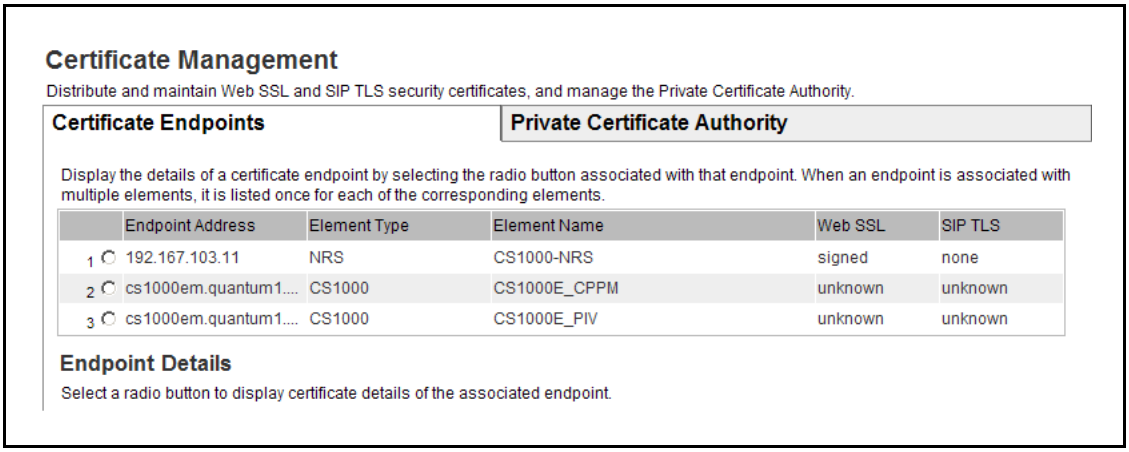
Procedure 43
Removing the current certificate by using UCM

Step	Action

1 Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.

2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints | Private Certificate Authority

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

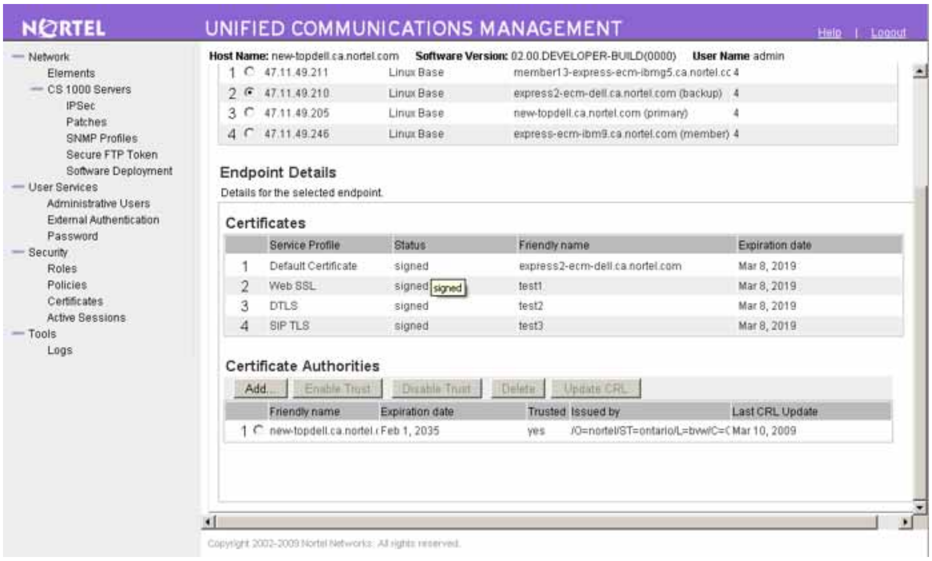
	Endpoint Address	Element Type	Element Name	Web SSL	SIP TLS
1 ○	192.167.103.11	NRS	CS1000-NRS	signed	none
2 ○	cs1000em.quantum1....	CS1000	CS1000E_CPPM	unknown	unknown
3 ○	cs1000em.quantum1....	CS1000	CS1000E_PIV	unknown	unknown

Endpoint Details

Select a radio button to display certificate details of the associated endpoint.

3 In the **Certificate Endpoints** tab, select the radio button next to the endpoint you want to configure.

The **Endpoint Details** section appears.



Host Name: new-topdell.ca.nortel.com **Software Version:** 02.00.DEVELOPER-BUILD(0000) **User Name** admin

1	○	47.11.49.211	Linux Base	member13-express-ecm-ibmg5.ca.nortel.cc	4
2	●	47.11.49.210	Linux Base	express2-ecm-dell.ca.nortel.com (backup)	4
3	○	47.11.49.205	Linux Base	new-topdell.ca.nortel.com (primary)	4
4	○	47.11.49.246	Linux Base	express-ecm-ibm9.ca.nortel.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	express2-ecm-dell.ca.nortel.com	Mar 8, 2019
2	Web SSL	signed signed	test1	Mar 8, 2019
3	DTLS	signed	test2	Mar 8, 2019
4	SIP TLS	signed	test3	Mar 8, 2019

Certificate Authorities

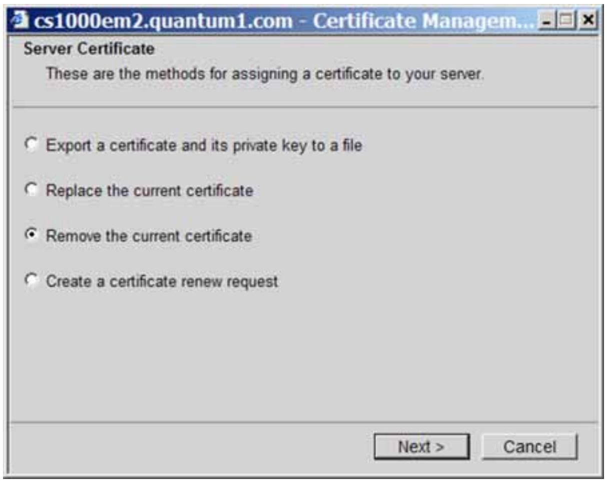
	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1 ○	new-topdell.ca.nortel.c	Feb 1, 2035	yes	/O=nortel/ST=ontario/L=bvw/C=C	Mar 10, 2009

Copyright 2002-2009 Nortel Networks. All rights reserved.

4 In the Endpoint Details pane, under Certificates, click **SIP TLS** or **Web SSL**.

The **Server Certificate** window appears.

The **Server Certificate** window appears.



cs1000em2.quantum1.com - Certificate Managem...

Server Certificate

These are the methods for assigning a certificate to your server.

○ Export a certificate and its private key to a file

○ Replace the current certificate

● Remove the current certificate

○ Create a certificate renew request

5 Select **Remove the current certificate**, and click **Next**.

The **Remove a Certificate** window appears.

6 Click **Finish**. The following message appears:
Web SSL and SIP TLS can be disrupted if no certificate is present. Therefore, if you remove the current certificate, you

must replace it or install a new one to prevent an interruption of service.

--End--

Revoke a certificate

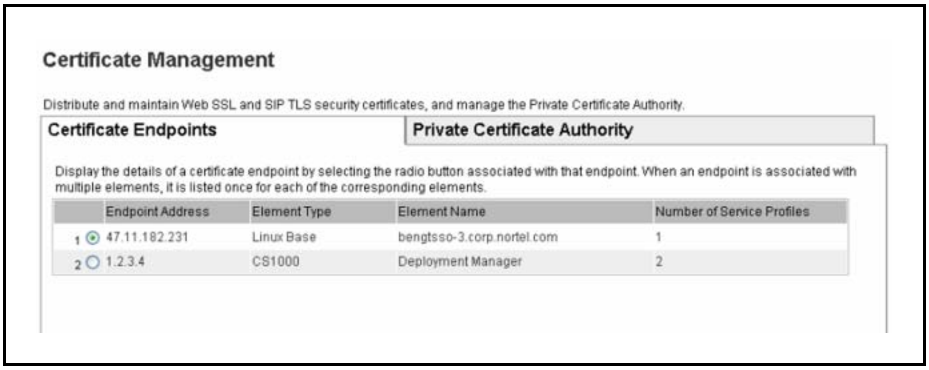
Use the following procedure to revoke a certificate.

Prerequisites

- You must have SecurityAdministrator privileges.

Procedure 44
Revoking a certificate

Step	Action
1	Log on to the UCM framework as a security administrator.
2	In the navigation tree, click **Security > Certificates** . The Certificate Management Web page appears.



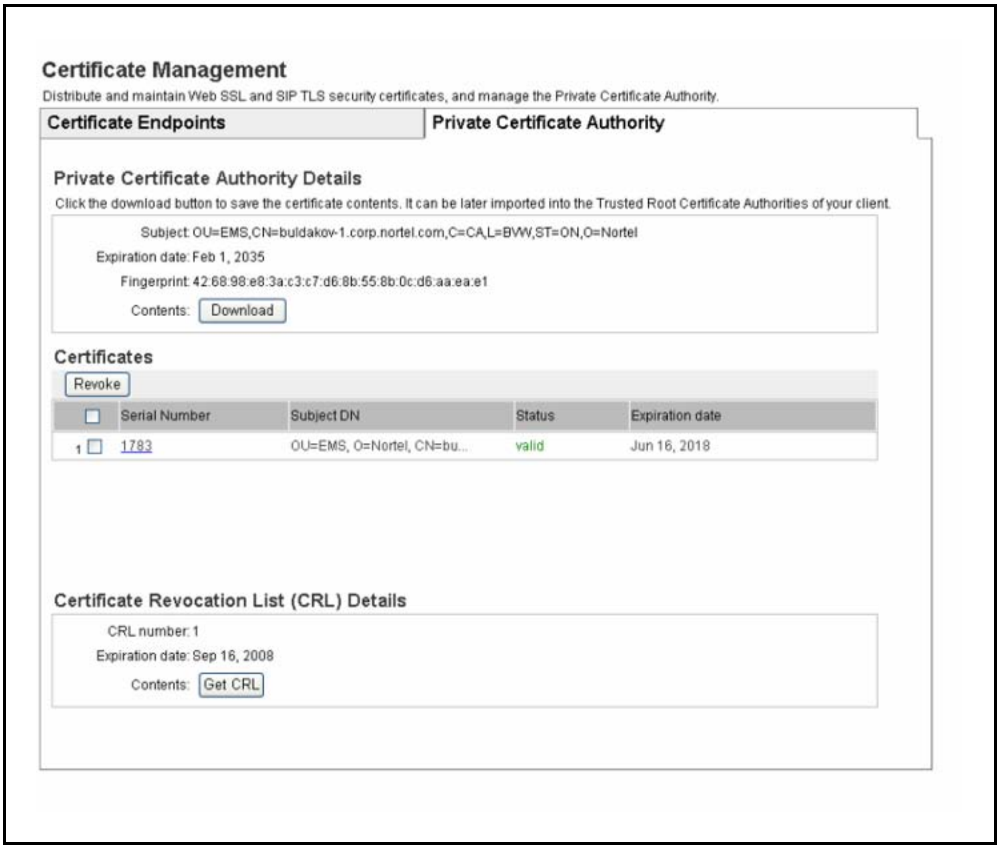
Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

3	Click the **Private Certificate Authority** tab. The Private Certificate Authority page displays.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Private Certificate Authority Details

Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities of your client.

Subject: OU=EMS,CN=buldakov-1.corp.nortel.com,C=CA,L=BVW,ST=ON,O=Nortel
Expiration date: Feb 1, 2035
Fingerprint: 42:68:98:e8:3a:c3:c7:d6:8b:55:8b:0c:d6:aa:ea:e1
Contents: Download

Certificates

Revoke

	☐	Serial Number	Subject DN	Status	Expiration date
1	☐	1783	OU=EMS, O=Nortel, CN=bu...	valid	Jun 16, 2018

Certificate Revocation List (CRL) Details

CRL number: 1
Expiration date: Sep 16, 2008
Contents: Get CRL

4 In the Certificates section, select one or more of the check boxes and click **Revoke** to revoke the selected certificates.

--End--

Download the Certificate Revocation List (CRL) Details

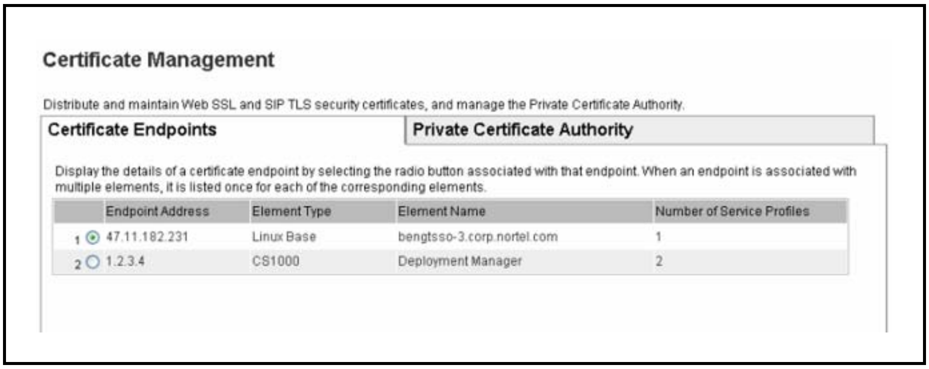
Use the following procedure to download the Certificate Revocation List (CRL) Details.

Prerequisites

- You must have SecurityAdministrator privileges.

Procedure 45
Downloading the Certificate Revocation List (CRL) Details

Step	Action
1	Log on to the UCM framework as a security administrator.
2	In the navigation tree, click **Security**, **Certificates**. The Certificate Management Web page appears.



Certificate Management

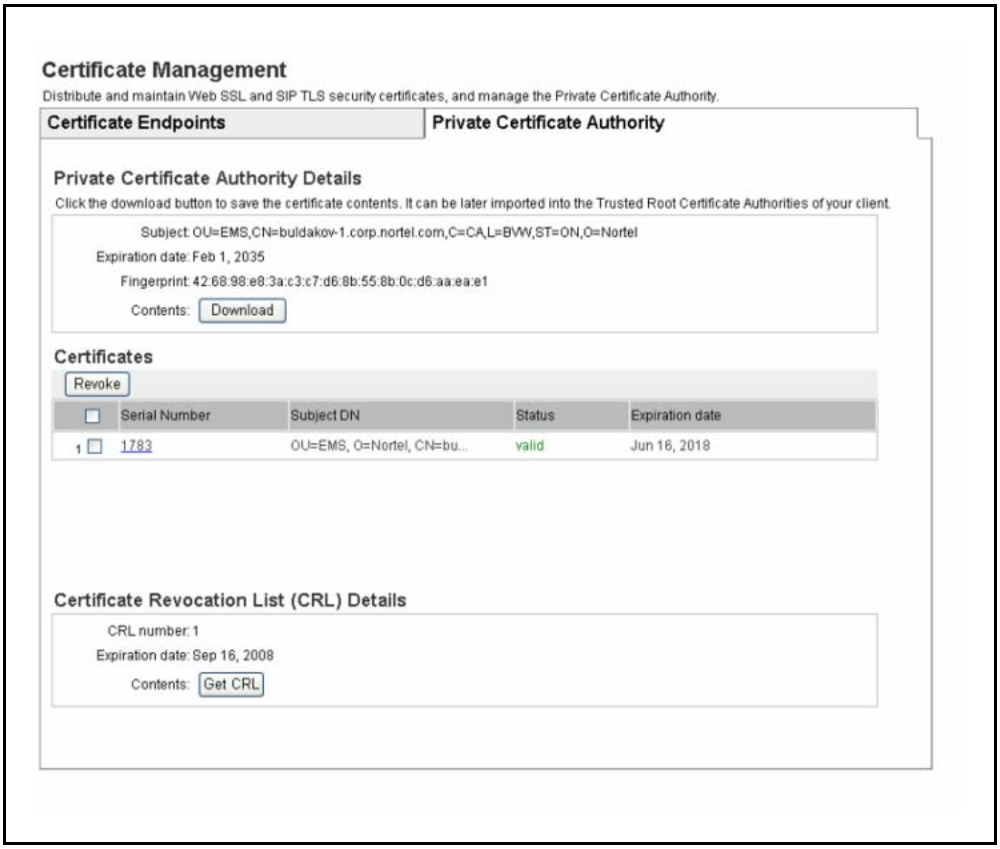
Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1 ●	47.11.182.231	Linux Base	bengtsso-3.corp.nortel.com	1
2 ○	1.2.3.4	CS1000	Deployment Manager	2

3 Click the Private Certificate Authority tab.

The Private Certificate Authority page displays.



Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Private Certificate Authority Details

Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities of your client.

Subject: OU=EMS,CN=buldakov-1.corp.nortel.com,C=CA,L=BVW,ST=ON,O=Nortel
Expiration date: Feb 1, 2035
Fingerprint: 42:68:98:e8:3a:c3:c7:d6:8b:55:8b:0c:d6:aa:ea:e1
Contents: Download

Certificates

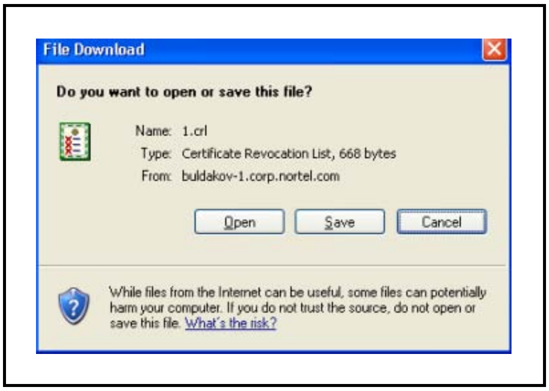
	Serial Number	Subject DN	Status	Expiration date
1 □	1783	OU=EMS, O=Nortel, CN=bu...	valid	Jun 16, 2018

Certificate Revocation List (CRL) Details

CRL number: 1
Expiration date: Sep 16, 2008
Contents: Get CRL

4 In the Certificate Revocation List (CRL) Details section, click **Get CRL**..

The File Download window appears.



File Download

Do you want to open or save this file?

Name: 1.crl

Type: Certificate Revocation List, 668 bytes

From: buldakov-1.corp.nortel.com

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

5 Click **Save**.

--End--

SIP security

This chapter contains procedures to help you protect Session Initiation Protocol (SIP) signaling by using Transport Layer Security (TLS). The chapter is divided into the following sections:

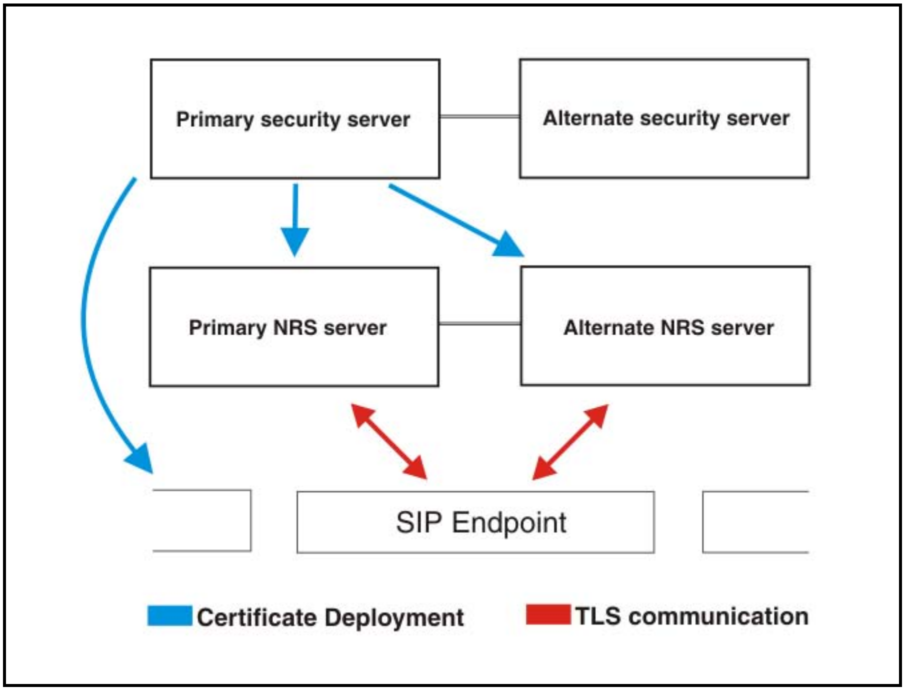
- “About TLS security for SIP trunks” (page 169)
- “SIP TLS configuration overview” (page 171)
- “TLS security for SIP trunks configuration using Element Manager” (page 175)
- “SIP TLS Certificate management” (page 181)
- “SIP TLS maintenance using CLI” (page 181)

About TLS security for SIP trunks

TLS protects SIP signaling traffic, providing message confidentiality and integrity in transit, as well as client-server authentication. Use the procedures in this section to configure SIP TLS on your system. For more information about SIP TLS concepts and implementation on Communication Server 1000, see “TLS security for SIP trunks concepts” (page 44).

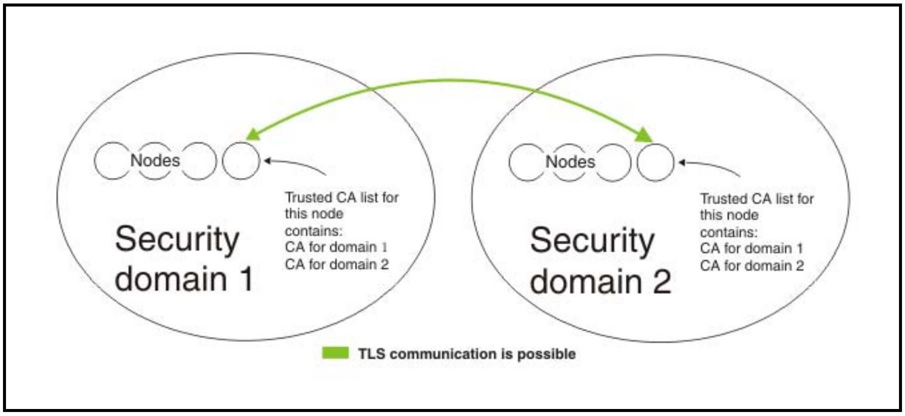
Certificates are deployed from the primary security server to the primary and secondary NRS servers and to the SIP endpoints. TLS communication can then be enabled between the active NRS server and the SIP endpoints. For an illustration of the distribution of certificates and subsequent TLS communication within a security domain, see .

Figure 8
SIP TLS with one security domain



To allow TLS communication between nodes on different security domains, you must add the Certificate Authorities (CA) for all of the security domains to the trusted CA list for each node that you want to allow to communicate using TLS. For an illustration of the distribution of CAs and subsequent communication between security domains, see the following figure.

Figure 9
SIP TLS with multiple security domains


Nodes
Trusted CA list for this node contains: CA for domain 1 CA for domain 2
Security domain 1
Nodes
Trusted CA list for this node contains: CA for domain 1 CA for domain 2
Security domain 2
TLS communication is possible

SIP Lines

SIP Lines operate similar to SIP trunks, however certificate installation for supported phone devices depends upon the specific device. For SIP Lines, the SIP Line Gateway (SLG) is updated with a certificate as opposed to the SIP Gateway used for SIP trunks.

For information about SIP Lines, see *SIP Line Fundamentals* (NN43001-508).

SIP TLS configuration overview

A typical deployment of a SIP-enabled Communication Server 1000 IP Peer network using SIP signaling consists of a Linux-based SIP Proxy and Redirect server or Linux-based NRS zone. Each such zone consists of one primary NRS, one secondary NRS, and multiple SIP gateway endpoints. The system must also include an Element Manager on Unified Communications Management that is the primary security server, and all the NRS must be members of the Unified Communications Management community of trust of that primary Unified Communications Management security server.

In the following example, you can use either SIP Proxy and Redirect servers or SIP endpoints as the system element. To configure SIP TLS, you must carry out the following four tasks.

1. Deploy certificates for SIP Proxy and Redirect server
   - In Unified Communications Management, create a certificate by using the steps in one of the following:
     - “Create a certificate for SIP TLS signed by the private CA ” (page 123)
     - “Create a certificate for SIP TLS signed by a public CA ” (page 128)
     - “Create a self-signed certificate for SIP TLS ” (page 140)
   - If the system has a secondary NRS with SIP Proxy and Redirect server:
     - In Unified Communications Management, select the server you configured in the steps above and export the certificate and the private key to a file by using the steps in “Export the current certificate and its private key” (page 153).
     - In Unified Communications Management, select the server to which you want to add the certificate, and Import a certificate

and its key by using the steps in "Import a certificate and its private key from a file" (page 156).

- In Unified Communications Management, add a CA to the service, and paste the certificate information by using the steps in "Add a CA to an endpoint" (page 99).

2. Enable TLS for SIP Proxy and Redirect server

   — If there is a firewall between the Unified Communications Management primary security server and the SIP Proxy and Redirect server, open the ports on the firewall to allow certificate communication, as follows:

     - TCP port 5061 for SIP TLS communication
     - UDP port 500 for IPsec Internet Key Exchange (IKE)
     - Protocol 50 for IPsec Encapsulated Payload Protocol (ESP)
     - TCP port 22 for SSH
     - TCP port 80 for HTTP
     - TCP port 443 for HTTPS
     - TCP port 58080 for SAML
     - TCP port 58081 for SAML secure mode
     - TCP port 636 for LDAPS
     - TCP port 15080 for Xmsg (only required if ISSS/IPsec disabled)

   — Complete the following steps only once for the system. You do not need to repeat them each time you configure TLS for a SIP endpoint:

     - In Unified Communications Management, provision a public-key certificate for the primary SIP Proxy and Redirect server
     - In Unified Communications Management, provision a public-key certificate for the secondary SIP Proxy and Redirect server
     - In NRS Manager, enable SIP Proxy to open TLS ports by using the information in *Network Routing Service Fundamentals* (NN43001-130).
     - Restart the SIP Proxy service.

3. Deploy certificates for SIP endpoints

   — In Unified Communications Management, create a certificate by using the steps in one of the following:

- "Create a certificate for SIP TLS signed by the private CA " (page 123)
- "Create a certificate for SIP TLS signed by a public CA " (page 128)
- "Create a self-signed certificate for SIP TLS " (page 140)

— If the system has other signaling servers running standby SIP services, you must perform the following steps for each signaling server:

- In Unified Communications Management, select the server you configured in the steps above and export the certificate and the private key to a file by using the steps in "Export the current certificate and its private key" (page 153).
- In Unified Communications Management, select the server to which you want to add the certificate, and Import a certificate and its key by using the steps in "Import a certificate and its private key from a file" (page 156).
- In Unified Communications Management, add a CA to the service, and paste the certificate information by using the steps in "Add a CA to an endpoint" (page 99).

4. Enable TLS for SIP endpoints

— If there is a firewall between the Unified Communications Management primary security server and the SIP endpoint, open the ports on the firewall to allow certificate communication, as follows:

- TCP port 5061 for SIP TLS communication
- TCP port for IPsec
- TCP port 22 for SSH
- TCP port 80 for HTTP
- TCP port 443 for HTTPS
- TCP port 58080 for SAML
- TCP port 58081 for SAML secure mode
- TCP port 636 for LDAPS
- TCP port 15080 for Xmsg

— In Element Manager, provision a SIP gateway to use TLS as transport protocol, save and transfer the changes, and restart the SIP Gateway by using the steps in "Configuring SIP TLS security policy" (page 176).

Use the command line interface (CLI) commands in “SIP TLS maintenance using CLI” (page 181) to check the configuration and status of the SIP/TLS connection.

View SIP TLS configuration

To view the current SIP TLS configuration, or to verify changes after you complete the procedures in this section, use the following procedure to examine the config.ini file.

Procedure 46
Viewing SIP TLS configuration

Step	Action
1	Log on to the SIP Gateway Signaling Server with an account that has PDT1 or PDT2 privilege.
2	Open the folder **`/u/config/`**.
3	Using a text editor, open the file **`config.ini`**. Compare the values in the file with those shown in “Job aid: config.ini” (page 174).

--End--

Job aid: config.ini

The system stores the SIP GW Settings configuration as follows:

```
[SIP GW Settings]
PrimaryProxyPort=5061
PrimaryProxyTransport=TLS
SecondaryProxyPort=5061
SecondaryProxyTransport=TLS
securityPolicy=1
tlsSecurityPort=5061
clientAuthenticationEnabled=0
numByteRenegotiation=20000000
x509CertAuthenticationEnabled=0
```

The values stored in the config.ini file are explained in Table 25 "SIP TLS security parameters" (page 175).

Table 25
SIP TLS security parameters

Parameter	Possible settings in Element Manager	Corresponding values in the config.ini file	Description
securityPolicy (Security Policy)	Security Disabled (Default) Best Effort Secure Local Secure End to End	0 = Security Disabled (Default) 1 = Best Effort 2 = Secure Local 3 = Secure End to End	Specify the security policy SIP TLS uses. For a description of each security policy, see Table 26 "Job aid: SIP TLS security policy descriptions" (page 178).
tlsSecurityPort (TLS Security Port)	A value in the range 1-65 535	Default value is : 5061	Enter the listening port that is used by TLS.
clientAuthenticationEnabled (Client Authentication)	Cleared / checked	0 = Disabled (Default) 1 = Enabled	Enable this option if you want both sides to authenticate; when it is disabled, authentication is one-way. If you enable this option, sessions require greater overhead.
numByteRenegotiation (Re-negotiation)	Cleared / checked	0 = Disabled 20 000 000 = Enabled (Default)	Enable this option if you want the session key used the SIP TLS connection to be renegotiated periodically. The default is Enabled; renegotiation is triggered after 20 000 000 bytes have passed over the connection.
x509CertAuthentication (X.509 Certificate Authentication)	Cleared / checked	0 = Disabled (Default) 1 = Enabled	Enable this option to cause SIP TLS to provide both encryption and identity verification. Disable this option to allow the system, when operating on the client side of the SIP/TLS connection, to accept self-signed certificates from the server side. If you disable x509CertAuthentication, the system provides encryption only (it does not verify identity).

TLS security for SIP trunks configuration using Element Manager

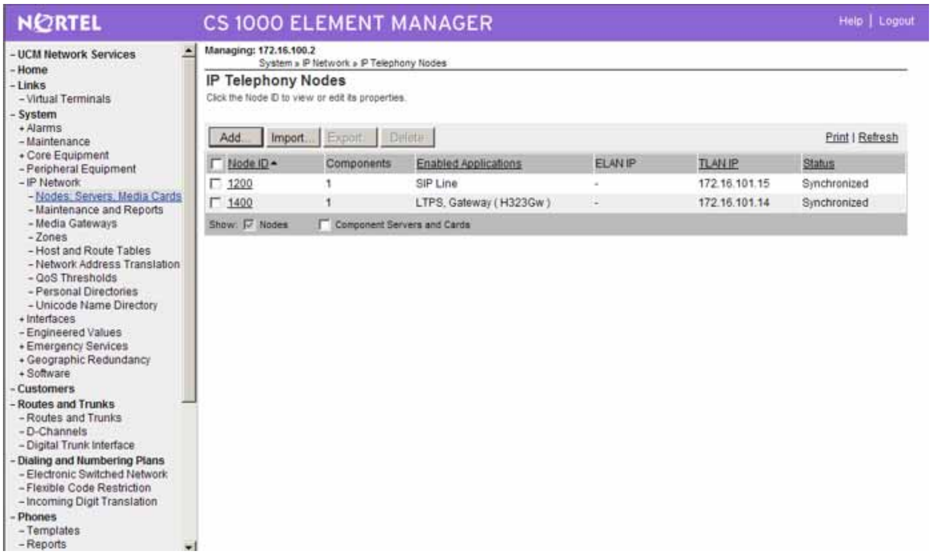
Use the procedures in this section to configure SIP TLS using Element Manager.

Configuring SIP TLS security policy

Use the procedures in this section to configure system-wide SIP TLS security policies.

Procedure 47
Configuring the system-wide TLS Security Policy by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **IP Telephony Nodes** page appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

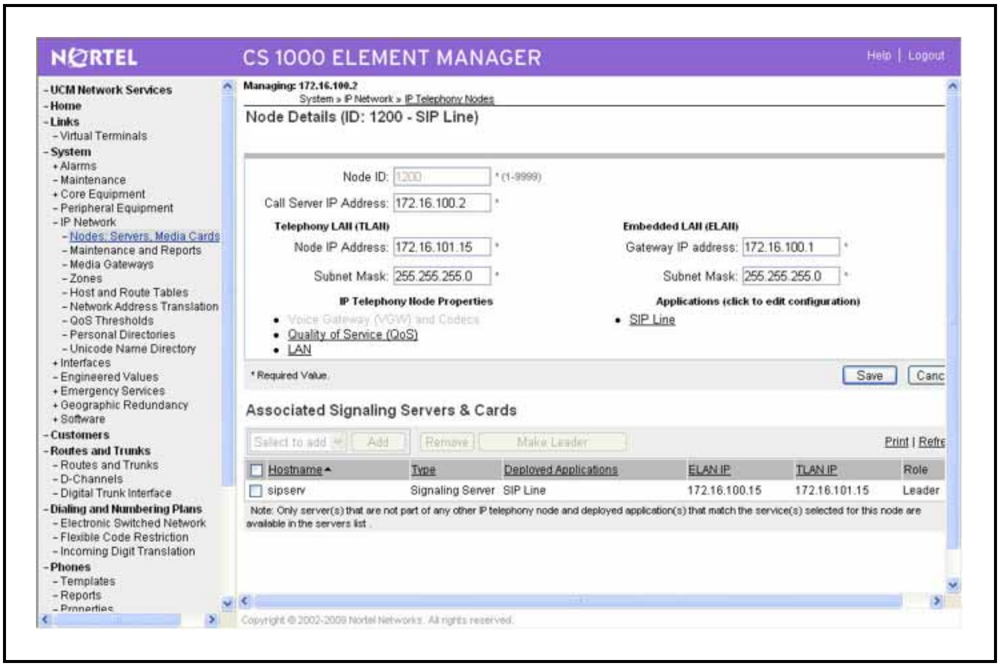
IP Telephony Nodes

Click the Node ID to view or edit its properties.

□	Node ID ▲	Components	Enabled Applications	ELAN IP	TLAN IP	Status
□	1200	1	SIP Line	-	172.16.101.15	Synchronized
□	1400	1	LTPS, Gateway (H323Gw)	-	172.16.101.14	Synchronized

Show: ☑ Nodes □ Component Servers and Cards

Step	Action
3	Click a Node ID to view the node properties.. The **Node Details** page appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node Details (ID: 1200 - SIP Line)

Node ID: 1200 * (1-9999)

Call Server IP Address: 172.16.100.2 *

Telephony LAN (TLAN)

Node IP Address: 172.16.101.15 *

Subnet Mask: 255.255.255.0 *

Embedded LAN (ELAN)

Gateway IP address: 172.16.100.1 *

Subnet Mask: 255.255.255.0 *

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

Applications (click to edit configuration)

- SIP Line

* Required Value.

Associated Signaling Servers & Cards

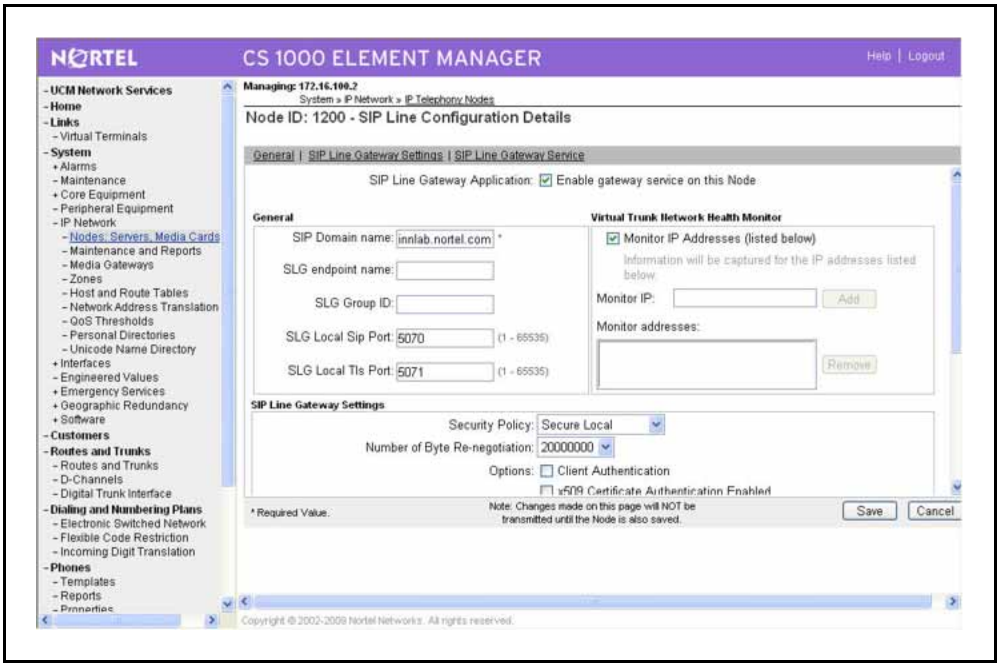
	Hostname	Type	Deployed Applications	ELAN IP	TLAN IP	Role
□	sipserv	Signaling Server	SIP Line	172.16.100.15	172.16.101.15	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

4 Under Applications, click **SIP Line**.

The SIP Line Configuration Details screen appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node ID: 1200 - SIP Line Configuration Details

SIP Line Gateway Application: ☑ Enable gateway service on this Node

General

SIP Domain name: innlab.nortel.com *

SLG endpoint name:

SLG Group ID:

SLG Local Sip Port: 5070 (1 - 65535)

SLG Local Tls Port: 5071 (1 - 65535)

Virtual Trunk Network Health Monitor

☑ Monitor IP Addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

SIP Line Gateway Settings

Security Policy: Secure Local

Number of Byte Re-negotiation: 20000000

Options: □ Client Authentication

□ x509 Certificate Authentication Enabled

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

5 In the General section, in the **SLG Local Tls Port** field, type `5061`.

For more information about TLS parameters, see Table 25 "SIP TLS security parameters" (page 175).

6 In the SIP Line Gateway Settings section, select a security policy from the **Security Policy** list menu. The options are as follows:

- **Security Disabled**
- **Best effort**
- **Secure Local**
- **Secure End to End**

For more information about available security policies, see Table 26 "Job aid: SIP TLS security policy descriptions" (page 178).

7 Optionally, select the **X509 Certificate Authentication** check box to enable X509 Certificate Authentication.

> **ATTENTION**
> If you select X509 Certificate Authentication, you cannot use self-signed certificates with SIP TLS.

8 Optionally, select the **Client Authentication** check box to enable Client Authentication.

9 Click **Save**.

The following warning appears:

```
Please reboot the following Signaling Server after
the save and transfer is done:  <list of SIP enabled
Signaling Servers IPs>.
```

10 Click **OK**.

--End--

The security policy options for SIP TLS are described in Table 26 "Job aid: SIP TLS security policy descriptions" (page 178).

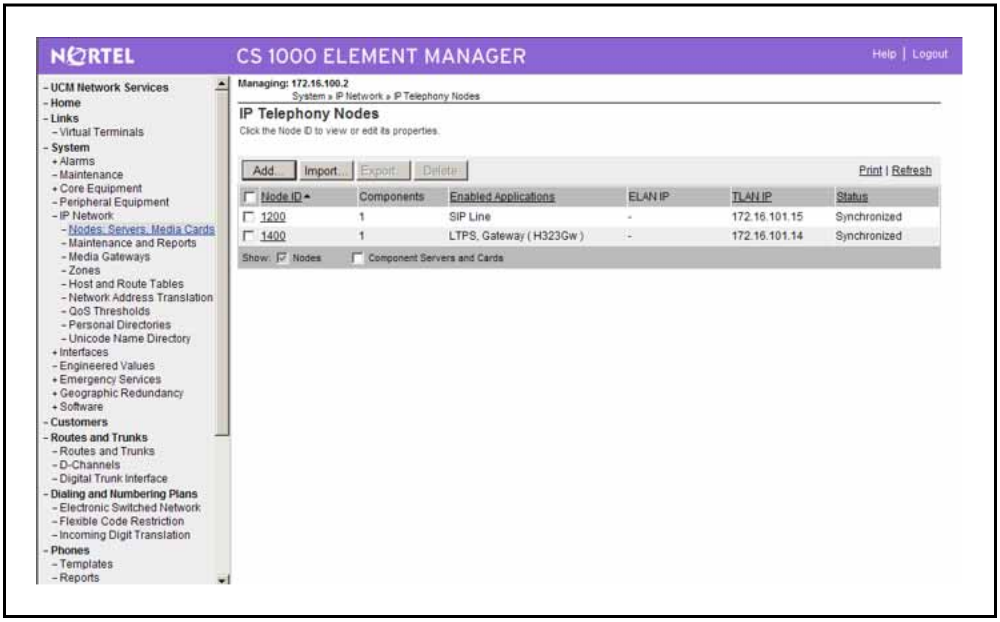
Table 26
Job aid: SIP TLS security policy descriptions

Security policy	Requirements
Security Disabled (No SIP TLS security)	Security Disabled turns SIP TLS off. SIP Gateway will listen on its TCP and UDP ports. Transport protocol to SIP Proxy or Redirect Server (for example, SIP Proxy and Redirect Server on Linux, and SIP Redirect Server on VxWorks) can be TCP or UDP. SIP URI scheme is SIP.
Best Effort (Best interoperability)	Best Effort turns SIP TLS on. SIP Gateway will listen on its TLS, TCP, and UDP ports. Transport protocol to SIP Proxy and Redirect Server on Linux can be TLS, TCP, or UDP. Transport protocol to SIP Redirect Server on VxWorks can be TCP or UDP. SIP URI scheme is SIP.

Secure Local (Guarantee local hop TLS)	Secure Local turns SIP TLS on. SIP Gateway will listen only on its TLS port. Transport protocol to SIP Proxy and Redirect Server on Linux can only be TLS. SIP Redirect Server on VxWorks is not supported as the next hop of this SIP Gateway. SIP URI scheme is SIP.
Secure End-to-End	Secure End-to-End turns SIP TLS on. SIP Gateway will listen only on its TLS port. Transport protocol to SIP Proxy and Redirect Server on Linux can only be TLS. SIP Redirect Server on VxWorks is not supported as the next hop of this SIP Gateway. SIP URI scheme is SIPS. In order to complete a call, all SIP Gateways in the network must be configured with Secure End-to-End , and all SIP Proxy Servers on Linux must be configured to support TLS.
Note: If you use Secure End-to-End policy or Secure Local policy, Failsafe Redirect Server is not supported.	

Procedure 48
Disabling SIP TLS by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **IP Telephony Node** page appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

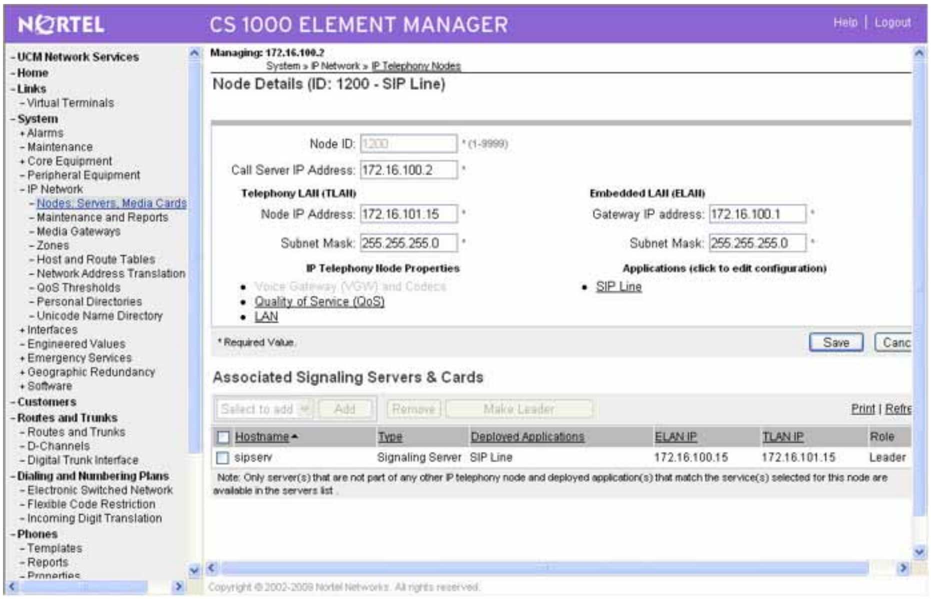
IP Telephony Nodes

Click the Node ID to view or edit its properties.

□ Node ID ▴	Components	Enabled Applications	ELAN IP	TLAN IP	Status
□ 1200	1	SIP Line	-	172.16.101.15	Synchronized
□ 1400	1	LTPS, Gateway (H323Gw)	-	172.16.101.14	Synchronized

Show: ☑ Nodes □ Component Servers and Cards

3	Click the link for the node you want to edit. The **Node Details** page appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node Details (ID: 1200 - SIP Line)

Node ID: 1200 * (1-9999)

Call Server IP Address: 172.16.100.2 *

Telephony LAN (TLAN)

Node IP Address: 172.16.101.15 *

Subnet Mask: 255.255.255.0 *

Embedded LAN (ELAN)

Gateway IP address: 172.16.100.1 *

Subnet Mask: 255.255.255.0 *

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

Applications (click to edit configuration)

- SIP Line

* Required Value.

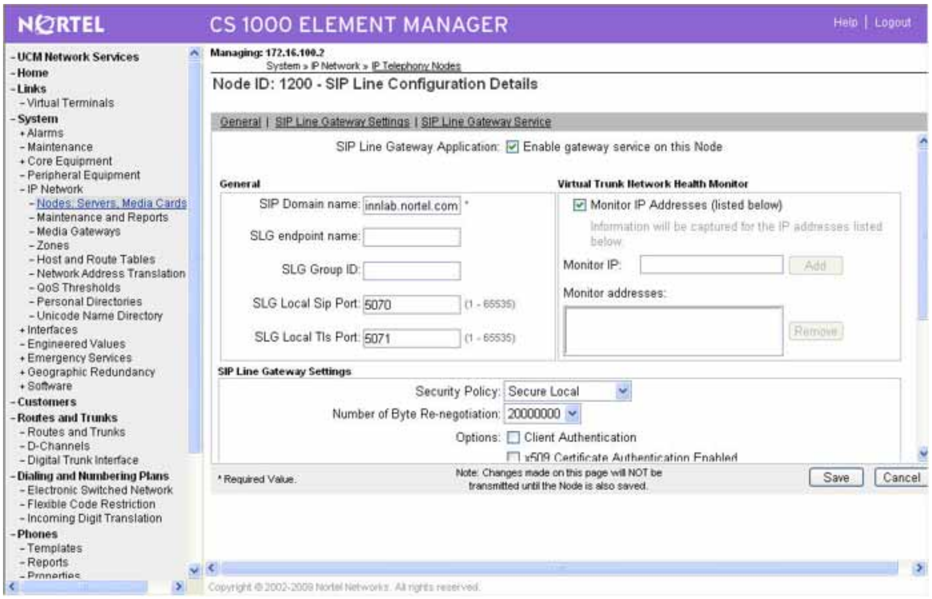
Associated Signaling Servers & Cards

□ Hostname	Type	Deployed Applications	ELAN IP	TLAN IP	Role
□ sipserv	Signaling Server	SIP Line	172.16.100.15	172.16.101.15	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

4 Under Applications, click **SIP Line**.

The SIP Line Configuration Details screen appears.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node ID: 1200 - SIP Line Configuration Details

SIP Line Gateway Application: ☑ Enable gateway service on this Node

General

SIP Domain name: innlab.nortel.com *

SLG endpoint name:

SLG Group ID:

SLG Local Sip Port: 5070 (1 - 65535)

SLG Local Tls Port: 5071 (1 - 65535)

Virtual Trunk Network Health Monitor

☑ Monitor IP Addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

SIP Line Gateway Settings

Security Policy: Secure Local

Number of Byte Re-negotiation: 20000000

Options: □ Client Authentication

□ x509 Certificate Authentication Enabled

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

5 In the SIP Line Gateway Settings section, select Security Disabled from the **Security Policy** list menu.

6 Verify that the **SLG Local Tls Port** , **Client Authentication**, **Re-negotiation**, and **X509 Certificate Authentication** areas are cleared.

For more information about TLS parameters, see Table 25 "SIP TLS security parameters" (page 175).

7 Ensure that all other fields on the page are configured with values appropriate to the SIP configuration on your system.

8 Click **Save**.

The following warning appears:
`Please reboot the following Signaling Server after the save and transfer is done: <list of SIP enabled Signaling Servers IPs>.`

9 Click **OK**.

--End--

You can verify the changes by checking the config.ini file [SIP GW Settings] section. For more information about verifying SIP TLS configuration changes, see "View SIP TLS configuration" (page 174).

SIP TLS Certificate management

You can manage SIP TLS certificates using the Unified Communications Management (UCM) interface. For more information about certificate management using Unified Communications Management, see "Certificate Management" (page 95).

SIP TLS maintenance using CLI

Use the following SIP Gateway serviceability commands at the command line interface (CLI) to display information about SIP TLS. To access these commands, you must log on using the PDT2 password on the Signaling Server. For more information about using these commands, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

- **`SIPGwShow`** You can use this command to display information including primary and secondary proxy transport types and TLS usage. The URI scheme appears in the channel table at the end of the output from this command.
- **`SIPCallTrace`** In addition to previous functionality, you can now use this command to show the transport and URI scheme.
- **`SIPTLSConfigShow`** Use this command to display TLS configuration parameters of the system as a whole, including client and server session caching parameters, the certificate for the local system, and the certificates that are configured.
- **`SIPTLSSessionShow`** Use this command to display the details of all SIP TLS sessions or sessions associated with a given server IP address. This command shows existing sessions (in connected state

and persistent), cached sessions, and the uptime and cipher suites, but does not show key information.

- **`SIPMessageTrace`** Use this command to configure filtering criteria for message tracing.

Media Security

This chapter contains procedures to help you protect the media stream by using the Media Security feature. The chapter is divided into the following sections:

- “About Media Security” (page 183)
- “UNIStim with DTLS encryption” (page 185)
- “Key sharing” (page 196)
- “Media Security configuration using Element Manager” (page 196)
- “Media Security configuration using overlays” (page 201)
- “Media Security configuration information” (page 205)

About Media Security

Use the Media Security feature to secure media exchanges on Communication Server 1000 through the use of Secure Real-time Transport Protocol (SRTP) on IP media paths. It applies to Communication Server 1000 IP Phones (Phase 2 only) and devices using DSPs (DSP daughterboard and MC32S).

With the SRTP feature you can encrypt media exchanges between two IP Phones. If you enable Media Security and a secure connection is established, IP Phones display a security icon, indicating that the leg of the call from the IP Phone to the first IP termination is secure.

SRTP cannot provide Media Security for conference calls hosted through Multimedia Application Server (MAS). For more information about Media Security concepts and implementation on Communication Server 1000, see “Media Security concepts” (page 42).

You can configure:

- a system-wide configuration setting that controls whether or not the CS 1000 system is capable of providing Media Security.
- a Media Security Class of Service on each IP Phone, which can have any of the following values: MSSD, Best Effort, Always, or Never.
- a system-wide Class of Service parameter for IP Phones, called Media Security System Default (MSSD). When you change the MSSD parameter, the system updates any IP Phones that have a Class of Service value of MSSD to use the new MSSD parameter. IP Phones that have a Class of Service other than MSSD are not affected when the system MSSD parameter is updated.

Table 27 "Configuration options available for Media Security" (page 184) shows the configuration possibilities for the Media Security feature.

Table 27
Configuration options available for Media Security

Endpoint Types	Never	Best Effort Secure IP	Always Secure IP
UNISTIM IP Phone	Y	Y	Y
TDM lines and trunks	Best Effort. No configuration option.		
VIRTUAL (SIP) Trunk (used for TDM originations)	Y	Y	N/A
SIP Endpoint	SIP Endpoint is configured in the IP Phone, not on the Call Server.		

For more information about Class of Service options for Media Security, see Table 28 "Details of Class of Service options for Media Security" (page 184).

Table 28
Details of Class of Service options for Media Security

Class of Service	Description
Always Secure IP (MSAW)	The IP Phone can engage in secure media exchanges only, both in the incoming and in the outgoing directions. For an outgoing call attempt, the Call Server offers Media Security to the terminator, and if the terminator accepts the offer, the media is secured by SRTP and a security icon is shown on the display, if applicable. If the terminator does not accept the offer, the call disconnects and a reorder tone sounds.

	The IP Phone rejects any incoming call attempt without a security offer and a reorder tone sounds.
Best Effort (MSBT)	The IP Phone can engage in secure media exchanges or insecure ones, depending on the capabilities of the IP Phone at the far end. On outgoing calls, the IP Phone attempts to originate secure calls, but falls back to RTP if the IP Phone at the far end is not capable of establishing a secure connection. If there is a security offer in the incoming call, the IP Phone accepts the offer and establishes SRTP streams; otherwise it establishes RTP streams. If applicable, icon is shown on the display when a secure connection is established.
Never (MSNV)	The IP Phone can engage in unsecured calls only. It does not propose security on outgoing calls and ignores SRTP offers for incoming calls. Use this setting if you want the IP Phone to work as it did with a previous release of CS 1000 software (for example, Release 5.5).
System Default (MSSD)	The IP Phone has a security setting as specified by the system-wide default parameter. Use this configuration option change the Class of Service settings for a group of IP Phones, without provisioning them one at a time. The system default value is one of Always, Best Effort, or Never.

The Best Effort security setting is sufficient to suit the security needs of most users. Apply the other settings on a case-by-case basis.

UNIStim with DTLS encryption

Secured UNIStim signal encryption is provided by Datagram Transport Layer Security (DTLS), which encrypts the data exchanges between the Signaling Server and the IP Phones. Previously, Secure Multimedia Controllers (SMC 2450) were required for UNIStim encryption, but DTLS requires no new additional hardware and can coexist with currently installed SMCs. You can configure DTLS and non-DTLS systems on the same network.

To enable DTLS encryption, the CS 1000 system must be upgraded to Release 6.0 and the IP Phones must have the latest firmware. Also, the system has to be configured with at least the Basic Security level.

> ***Note:*** This feature does not provide signaling encryption for the UFTP protocol, which is used when transferring firmware to IP Phones. Firmware data contains no sensitive information and is protected from third-party tampering by a digital signature. Notifications from the signaling server to the phones are sent using DTLS-protected UNIStim signaling to protect the signals from intercept.

The UNIStim security with DTLS feature allows the Signaling Server to detect if an IP Phone is using Secure UNIStim. You can then list IP Phones based on their employed encryption type by using the isetSecGet command on the Signaling Server or the STIP DTLS command in overlay 117 on the Call Server.

Due to the implementation of the UNIStim proxy in the Secure Multimedia Controller, it is not possible for the Signaling Server to switch the phones protected by Secure UNIStim to DTLS. You must change the action byte setting on those phones to use DTLS instead of USec, which you can do manually on the client side or by using the isetSecUpdate command on the server side.

If the configuration is provisioned to the IP Phones by DHCP or a Provisioning Server, those servers must be updated. The DTLS signaling uses different UDP ports from those used by insecure RUDP, so you must configure the network firewalls (including SMC) to allow traffic on UDP ports 4101, 7301, and 5101.

DTLS and IP Phone registration

There are two modes of IP Phone registration:

- Secure Handshake mode—the IP phone is configured to initiate a DTLS session immediately upon beginning registration.
- Switchover mode—the IP phone is configured to first establish an unencrypted RUDP session to the LTPS, then switchover to DTLS depending on the DTLS Policy

Supported hardware

UNIStim with DTLS is supported on the following Communication Server 1000 components:

- **Call Servers**
  - CP PIV
  - CP PM (Standalone)
  - CP PM (Co-resident)
- **Signaling Servers**
  - CP PM (Standalone)
  - CP PM (Co-resident)
  - HP DL320 G4
  - IBM x306m

- IBM x3350
- Dell R300

Currently, the following IP Phones support DTLS signaling encryption (after applicable firmware upgrade):

> **ATTENTION**
> IP Phones require UNIStim 4.0 or later to support DTLS signaling encryption.

- IP Phone 1200 series (IP Phone 1210, IP Phone 1220, IP Phone 1230)
- IP Phone 1100 series (IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E)
- IP Phone 2000 series (IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007)

Security levels

Various configuration options of UNIStim with DTLS can be combined to form three security levels: Basic, Advanced, and Complete. As the level of security increases, there are certain limitations on the supported hardware and software.

> ***Note:*** You must configure the security levels sequentially. For example, to configure or upgrade the network to Complete security, you must first enable Basic security, then upgrade to Advanced security, and then upgrade to Complete security.

Table 29 "UNIStim with DTLS security levels" (page 187) lists the security levels and their descriptions.

Table 29
UNIStim with DTLS security levels

Security level	Description
Basic	This level provides average signaling security when both the IP Phone and LTPS support DTLS and does not introduce any feature limitations. All features, including Virtual Office, Branch Office and Geographic Redundancy, continue to work normally as without signaling encryption. You can select this level when most CS 1000 systems on the network are upgraded to Communication Server Release 6.0 and are configured for DTLS but there are systems which do not support DTLS (such as SRG or BCM) or which are not yet upgraded to 6.0. The DTLS policy on the Communication Server 1000 Release 6.0 systems is configured as DTLS Best Effort. Phones are configured with action byte 1. (USec-capable phones behind an SMC may be configured with action byte 6).

Security level	Description
	There is a brief period of insecure signaling at the beginning of registration.
Advanced	This level provides good security for sites requiring more than Basic security. You can use this configuration when all systems in the network are DTLS-enabled and configured as DTLS Best Effort. DTLS-capable phones are configured with action byte of 7 (regardless of whether they are behind an SMC or not). DTLS-incapable but USec-capable phones behind SMCs are configured with action byte of 6. DTLS-incapable phones which are not behind an SMC and those phones which are USec-incapable are configured with action byte of 1.
Complete	This level provides the best security for sites requiring all information on the network to be encrypted. All systems in the network are DTLS-enabled and configured as DTLS Always. All IP Phones are DTLS-capable and configured with action byte 7. Insecure registrations are not permitted.

DTLS configuration options

On the Communication Server 1000 system, DTLS-related behavior is controlled by a tri-state setting called Node DTLS Policy. This setting is configured by Line TPS node rather than on an individual system or element basis. The possible values are DTLS Off (default), DTLS Best Effort, and DTLS Always.

The DTLS policy controls which ports are open on the elements of the node and whether the elements will attempt to switch DTLS-capable phones to DTLS if they attempt to register insecurely.

Table 30
DTLS Call Server policies

	DTLS Off	DTLS Best Effort	DTLS Always
Insecure ports (4100, 7300, 5100)	Open	Open	Closed
Secure ports (4101, 7301, 5101)	Closed	Open	Open
Switchover	No switchover as DTLS is not enabled	DTLS-capable phones are switched to DTLS during registration	Registrations are only possible over DTLS, so no switchover is necessary.

Other available configuration options are Client Authentication and Renegotiation.

Client Authentication determines whether the LTPS requires a certificate to be sent from the IP clients for mutual authentication.

Renegotiation determines whether the DTLS connection is refreshed periodically (re-keyed). The SIP TLS strategy of re-keying on a traffic threshold of 20,000,000 is followed if this setting is enabled.

All settings can be changed using the Node Properties page of Element Manager, which is accessed by navigating to **System > IP Network > Nodes: Servers, Media Cards**.

IP clients are configured with an action byte for each of the two servers (S1 and S2) to which the phone can register. The action byte dictates which protocol the phone should use to connect to the signaling server. This action byte is extended with a new value to indicate that the phone should use DTLS and should initiate a DTLS session with the server. Table 31 "DTLS action byte values for IP clients" (page 189) displays the possible action byte values.

Table 31
DTLS action byte values for IP clients

Action byte	Protocol stack	Note
1	UNIStim RUDP UDP	The IP Phone registers using UNIStim over RUDP, which is active over UDP. If the target LTPS node has “DTLS Best Effort” policy, the phone is switched to DTLS during registration (if it is DTLS-capable).
6	Secure UNIStim RUDP UDP	The IP Phone initiates secure UNIStim communication and establishes a secure channel with the Secure Multimedia Controller. All signaling messages, including registration messages, are protected by secure UNIStim. The LTPS detects the phones which are using Secure UNIStim and does not attempt to switch those phones to DTLS.
7	UNIStim RUDP DTLS UDP	The IP Phone initiates DTLS communication with the Signaling Server. After the DTLS session is established, the phone can register normally but uses UNIStim over DTLS. All signaling messages, including registration messages, are protected by DTLS. If the phone is configured with this action byte value, it will never be switched to Secure UNIStim or regular UNIStim.

UNIStim DTLS overlay commands

Use the STIP DTLS command in LD 117 to print information about IP Phones filtered by signaling encryption related values, including the type of connection the phone is currently using and the phones capability of making DTLS connections.

The syntax of the command is as follows:

```
STIP DTLS <NODE> <CONNECTION TYPE> <DTLS_CAPABILITY>
```

Parameter	Description
<NODE>	Node ID the phone belongs to, or use ALL to omit the node-based filtering
<CONNECTION_TYPE>	The following options are available: • INSECURE—prints the phones which are not using signalling encryption • SECURE—prints the phones which are using either USec or DTLS • DTLS—prints only the phones which are using DTLS • USEC—prints only the phones which are using UNIStim Security • ALL—prints all types of phones
<DTLS_CAPABILITY>	The following options are available: • YES—prints DTLS-capable phones • NO—prints non-DTLS capable phones • ALL—prints both DTLS and non-DTLS capable phones

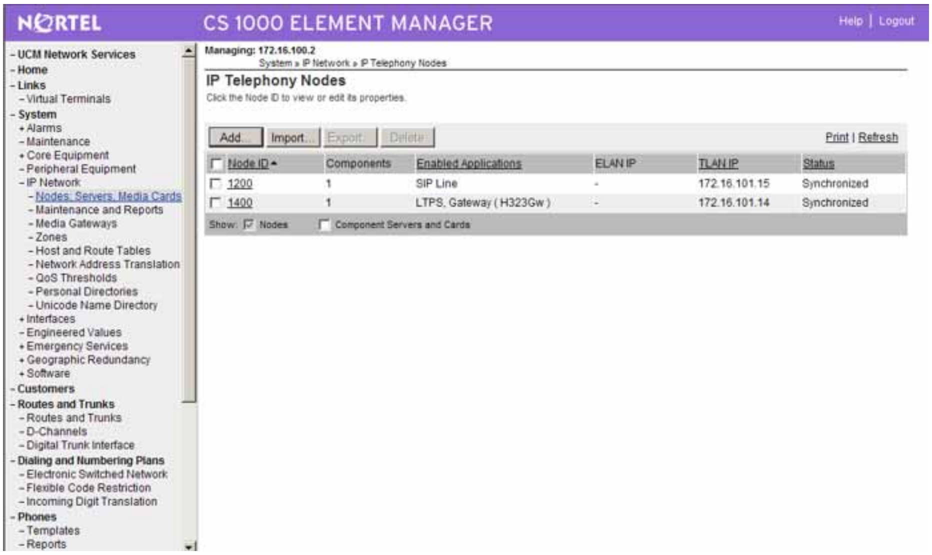
You can perform mass configuration of the S1 and S2 action byte values using the Iset command **isetSecUpdate**. For information about Iset commands, see Table 33 "Job aid: Iset commands for UNIStim DTLS" (page 194).

Configure UNIStim DTLS using Element Manager

Use the following procedure to configure UNIStim DTLS using Element Manager.

Procedure 49
Configuring UNIStim DTLS using Element Manager

Step	Action
1	Navigate to **System > IP Network > Nodes: Servers, Media Cards** page. The IP Telephony Nodes page displays.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

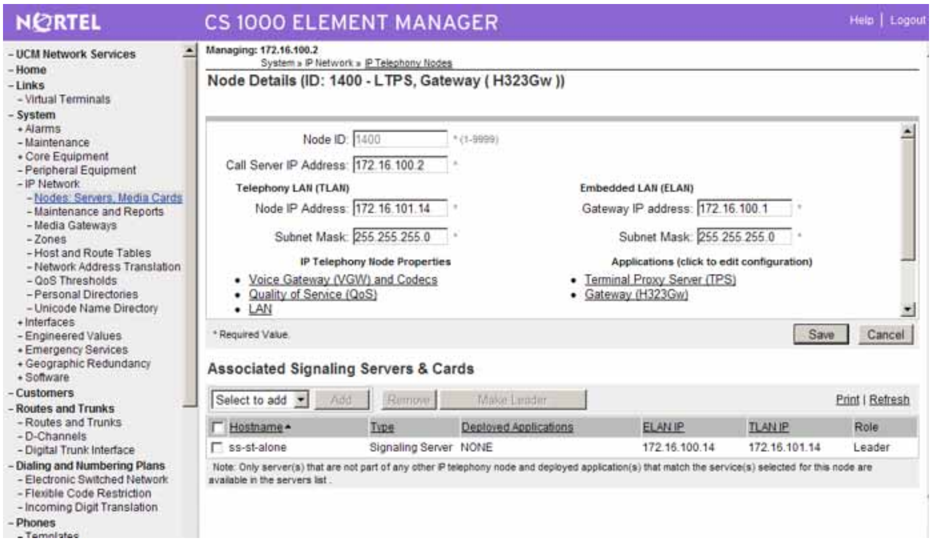
Click the Node ID to view or edit its properties.

□ Node ID	Components	Enabled Applications	ELAN IP	TLAN IP	Status
□ 1200	1	SIP Line	-	172.16.101.15	Synchronized
□ 1400	1	LTPS, Gateway (H323Gw)	-	172.16.101.14	Synchronized

Show: ☑ Nodes □ Component Servers and Cards

2 Click the hyperlink for the node you wish to configure.

The Node Details page displays.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node Details (ID: 1400 - LTPS, Gateway (H323Gw))

Node ID: 1400 * (1-9999)

Call Server IP Address: 172.16.100.2 *

Telephony LAN (TLAN)

Node IP Address: 172.16.101.14 *

Subnet Mask: 255.255.255.0 *

Embedded LAN (ELAN)

Gateway IP address: 172.16.100.1 *

Subnet Mask: 255.255.255.0 *

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

Applications (click to edit configuration)

- Terminal Proxy Server (TPS)
- Gateway (H323Gw)

* Required Value.

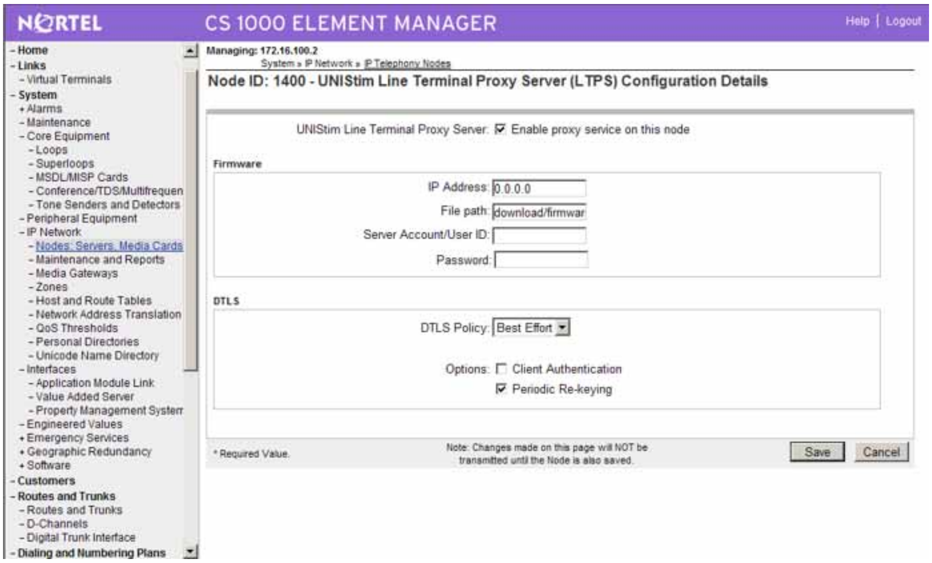
Associated Signaling Servers & Cards

□ Hostname	Type	Deployed Applications	ELAN IP	TLAN IP	Role
□ ss-st-alone	Signaling Server	NONE	172.16.100.14	172.16.101.14	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

3 Click the **Terminal Proxy Server (TPS)** hyperlink.

The Node ID * UNIStim Line Terminal Proxy Server (LTPS) Configuration Details page displays.



Managing: 172.16.100.2
System » IP Network » IP Telephony Nodes

Node ID: 1400 - UNIStim Line Terminal Proxy Server (LTPS) Configuration Details

UNIStim Line Terminal Proxy Server: ☑ Enable proxy service on this node

Firmware

IP Address: 0.0.0.0

File path: download/firmwar

Server Account/User ID:

Password:

DTLS

DTLS Policy: Best Effort

Options: ☐ Client Authentication
☑ Periodic Re-keying

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

The following items are listed in the DTLS section of the TPS configuration page:

- DTLS Policy
- Options

4 From the **DTLS Policy** list, select the desired DTLS Policy.

5 If you want to enable Client Authentication, select the **Client Authentication** check box.

6 If you want to enable Periodic Re-keying, select the **Periodic Re-keying** check box.

7 Click **Save**.

The configuration changes are saved and the Node Details page displays.

8 Click **Save** to save the new configuration details for the node.

--End--

Table 32
Job aid: DTLS parameters in Element Manager Node Configuration page

Parameter	Function	Description
DTLS Policy	Enables or disables DTLS	• OFF—DTLS is not active on the node and DTLS ports are closed. • Best Effort—Both DTLS and non-DTLS ports are open on elements. The node will accept both

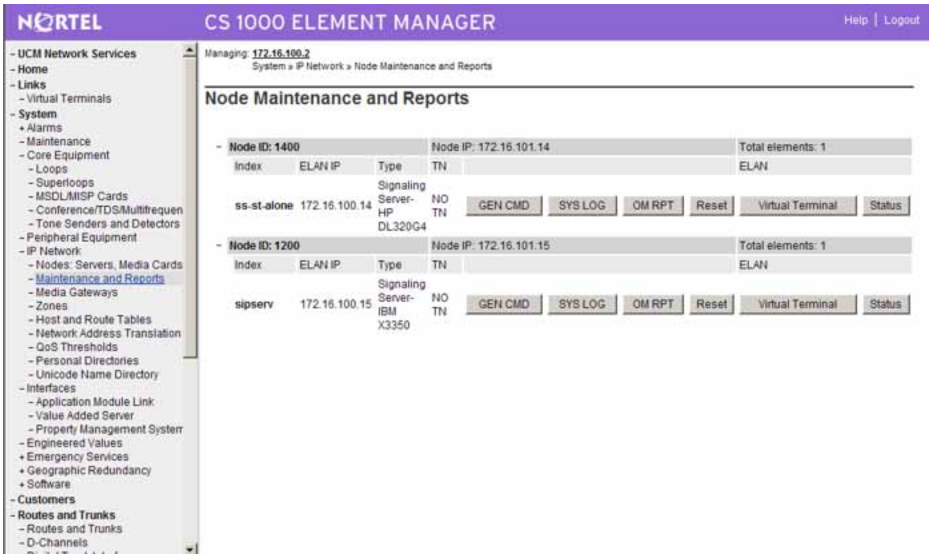
Parameter	Function	Description
		secure and insecure registrations and will attempt to switch capable phones to DTLS. - Always—The node accepts only secure registrations. Insecure RUDP ports are not open on the node elements. It is not possible to register a DTLS-incapable phone to this node.
Client Authentication	IP clients for mutual authentication	If selected, the server verifies client certificates and rejects registrations if certificates are invalid.
Periodic Re-keying	Periodically refresh (re-key) DTLS connection	If selected, periodic re-keying is enabled.

Update UNIStim DTLS using Element Manager

Use this procedure to retrieve and update the UNIStim DTLS information from an existing cluster.

Procedure 50
Updating UNIStim DTLS using Element Manager

Step	Action
1	In Element Manager, navigate to **System > IP Networks > Maintenance and Reports** . The Node Maintenance and Reports page displays.



Managing: 172.16.100.2
System » IP Network » Node Maintenance and Reports

Node Maintenance and Reports

- Node ID: 1400			Node IP: 172.16.101.14	Total elements: 1
Index	ELAN IP	Type	TN	ELAN
ss-st-alone	172.16.100.14	Signaling Server-HP DL320G4	NO TN	

- Node ID: 1200			Node IP: 172.16.101.15	Total elements: 1
Index	ELAN IP	Type	TN	ELAN
sipserv	172.16.100.15	Signaling Server-IBM X3350	NO TN	

You can click the **+** or **-** to expand or collapse the node details.

2	Choose the desired element and click **GEN CMD**.

3 From the Group list, select **Iset**.

4 From the Command list, select a command.

Refer toTable 33 "Job aid: Iset commands for UNIStim DTLS" (page 194) for a list of iset commands and their descriptions.

5 If applicable, enter the appropriate parameters for the selected command.

6 Click **Run**.

--End--

Table 33
Job aid: Iset commands for UNIStim DTLS

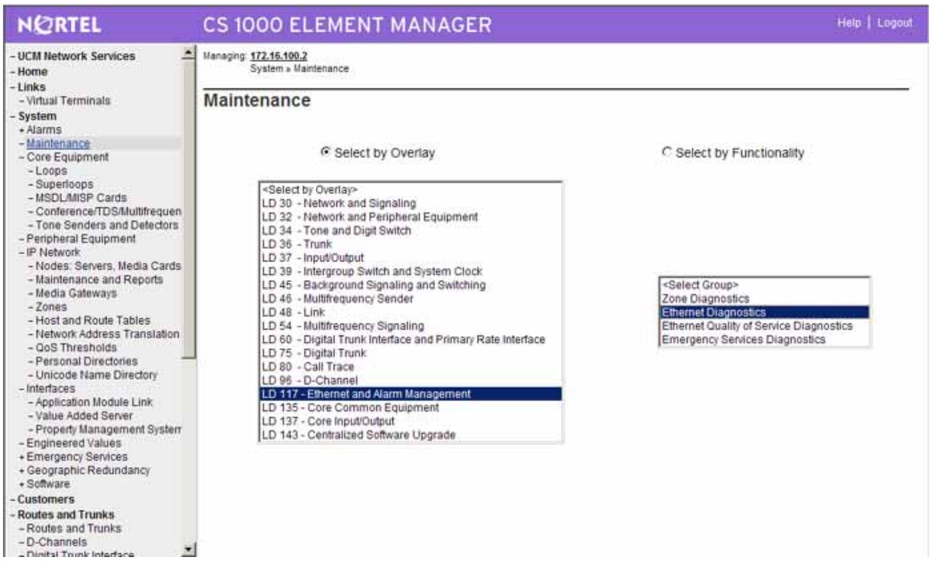
Command	Description
isetSecGet	Retrieves the DTLS IP Phone details, where: • Filter = a text string of one or more of the following filtering items: — IP — Type — TN — Encryption — Action — DTLSCap The filter field is limited to 80 characters.
isetSecUpdate	Reconfigures the S1 and S2 ports and action bytes on the IP Phones, where: • Filter = the same syntax as described for isetSecGet • Server ID = 1 or 2, to indicate whether S1 or S2 configurations must be updated • Action = 1, 6 or 7 • Port = the port number to be configured. The default port value is 4100 if Action is 1 or 6, and 4101 if Action is 7. Generally, it is not recommended to specify this value unless there is a need to do so.
isetSecUpdateShow	Prints the result of the isetSecUpdate command.
isetSecShow	Prints the DTLS IP Phone details.

View UNISTIM DTLS details using Element Manager

Use this procedure to retrieve and view the UNIStim DTLS details using the Element Manager interface. This procedure uses the same query as the STIP DTLS command in LD 117.

Procedure 51
Viewing UNIStim DTLS details using Element Manager

Step	Action
1	In Element Manager, navigate to **System > Maintenance**.
2	From the list, select **LD117 – Ethernet and Alarm Management**.
3	From the group menu, select **Ethernet Diagnostics**.



Managing: 172.16.100.2
System » Maintenance

Maintenance

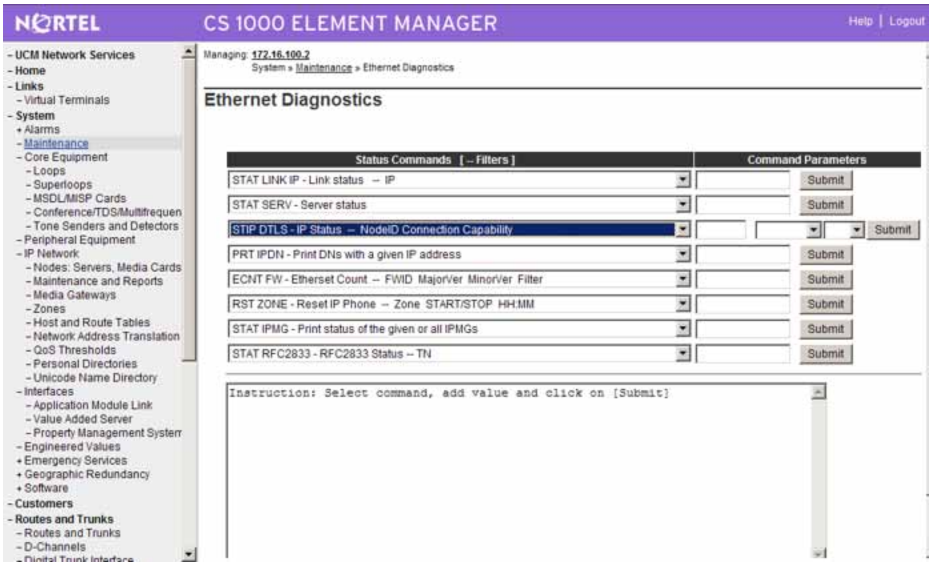
● Select by Overlay ○ Select by Functionality

<Select by Overlay>
LD 30 - Network and Signaling
LD 32 - Network and Peripheral Equipment
LD 34 - Tone and Digit Switch
LD 36 - Trunk
LD 37 - Input/Output
LD 39 - Intergroup Switch and System Clock
LD 45 - Background Signaling and Switching
LD 46 - Multifrequency Sender
LD 48 - Link
LD 54 - Multifrequency Signaling
LD 60 - Digital Trunk Interface and Primary Rate Interface
LD 75 - Digital Trunk
LD 80 - Call Trace
LD 96 - D-Channel
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>
Zone Diagnostics
Ethernet Diagnostics
Ethernet Quality of Service Diagnostics
Emergency Services Diagnostics

The Ethernet Diagnostics page displays.

4	From the STIP command list, select **STIP DTLS** .



Managing: 172.16.100.2
System » Maintenance » Ethernet Diagnostics

Ethernet Diagnostics

Status Commands [-- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SERV - Server status	Submit
STIP DTLS - IP Status -- NodeID Connection Capability	Submit
PRT IPDN - Print DNs with a given IP address	Submit
ECNT FW - Ethernet Count -- FWID MajorVer MinorVer Filter	Submit
RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM	Submit
STAT IPMG - Print status of the given or all IPMGs	Submit
STAT RFC2833 - RFC2833 Status -- TN	Submit

```
Instruction: Select command, add value and click on [Submit]
```

5 Enter the applicable Command Parameters.

6 Click **Submit**.

--End--

Key sharing

This section describes available types of key sharing. Keys must be either preshared, or exchanged over a secure UNIStim channel when needed by the system.

Protecting the media stream using SRTP PSK

SRTP using preshared key (PSK) does not require Call Server support, and therefore is useful for telephony environments where the installed Call Server software does not offer SRTP support.

To use this feature, SRTP (PSK) must be supported on each IP Phone in a call, and you must enable it on each IP Phone using the manual configuration menu. For more information about configuring SRTP (PSK), see *IP Phones Fundamentals* (NN43001-368).

Protecting the media stream using SRTP USK

SRTP using UNIStim Keys (USK) exchanges keys through UNIStim, using a secure channel.

To use this feature, SRTP (USK) must be supported on each IP Phone in a call, and must be supported by the Call Server. For more information about configuring SRTP (USK), see *IP Phones Fundamentals* (NN43001-368).

Media Security configuration using Element Manager

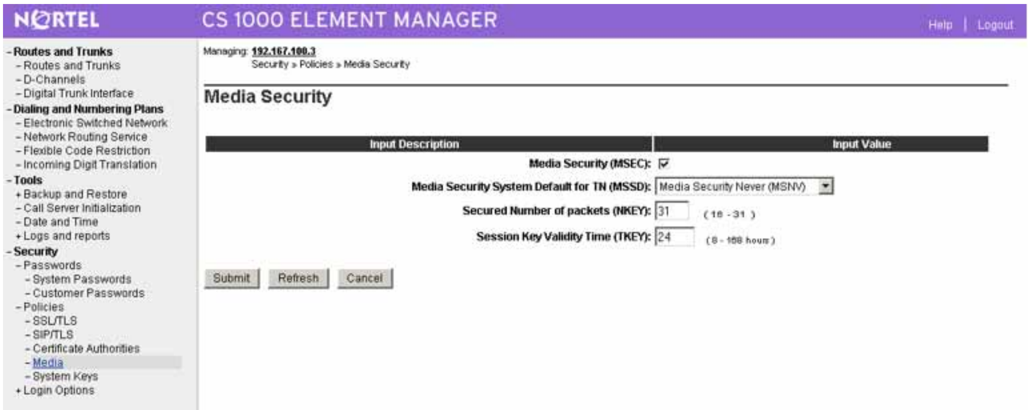
Use the procedures in this section to configure Media Security using Element Manager.

System-wide Media Security configuration

You can configure a system-wide configuration setting that controls whether or not the Communication Server 1000 system is capable of providing Media Security. By default, Media Security is enabled on the system.

You can configure system-wide Media Security using the Media Configuration page in Element Manager, as shown in Figure 10 "Media Security configuration" (page 197). For more information about configuring Element Manager, see *Element Manager System Reference — Administration* (NN43001-632).

Figure 10
Media Security configuration



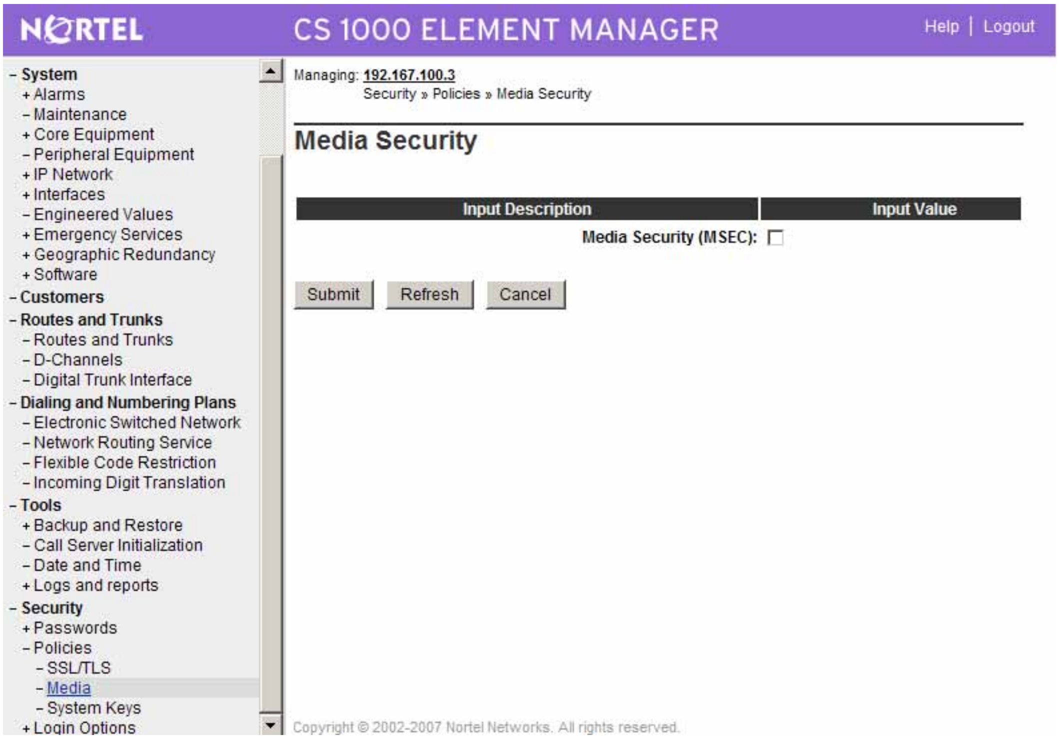
Managing: 192.167.100.3
Security » Policies » Media Security

Media Security

Input Description	Input Value
Media Security (MSEC):	☑
Media Security System Default for TN (MSSD):	Media Security Never (MSNV)
Secured Number of packets (NKEY):	31 (16 - 31)
Session Key Validity Time (TKEY):	24 (8 - 168 hours)

Procedure 52
Configuring system-wide Media Security by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Policies > Media** . The **Media Security** page appears.

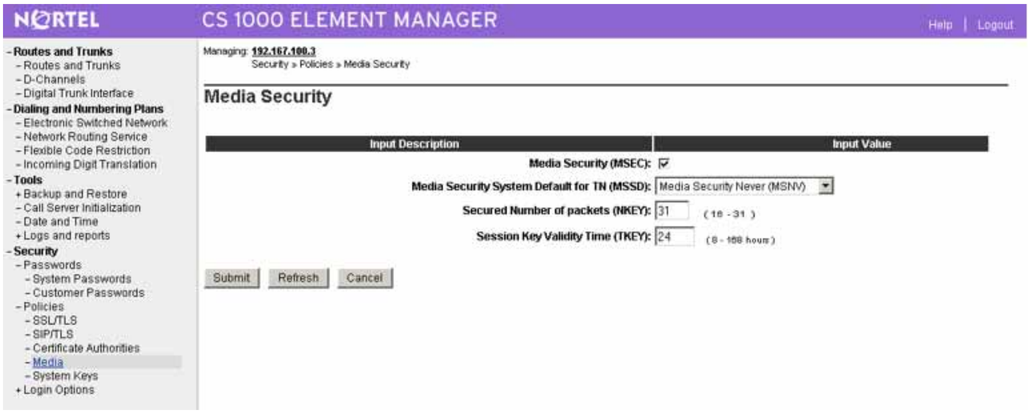


Managing: 192.167.100.3
Security » Policies » Media Security

Media Security

Input Description	Input Value
Media Security (MSEC):	□

3 Select the **Media Security** check box to enable system-wide Media Security.



Managing: 192.167.100.3
Security » Policies » Media Security

Media Security

Input Description	Input Value
Media Security (MSEC):	☑
Media Security System Default for TN (MSSD):	Media Security Never (MSNV)
Secured Number of packets (NKEY):	31 (16 - 31)
Session Key Validity Time (TKEY):	24 (8 - 168 hours)

4 Choose one of the following options from the **Media Security System Default for TN** menu:

MSNV to configure the Media Security default value to Never, which disables Media Security on all TNs that have the security Class of Service configured as MSSD.

OR

MSBT to configure the Media Security default value to Best Effort, which configures Media Security to use Best Effort on all TNs that have the security Class of Service configured as MSSD.

OR

MSAW to configure the system-wide default value to Always, which configures Media Security to allow secure media exchanges only. Unsecured connection attempts are blocked.

5 Enter a value in the **Secured Number of packets (NKEY)** field. The value you enter configures the number of packets a key can secure before it must be regenerated, and must be an integer in the range of 16 to 31.

6 Enter a value in the **Session Key Validity Time (TKEY)** field. The value you enter configures the maximum length of time, in hours, that a session key can remain valid, and must be an integer in the range of 8 to 168.

7 Click **Submit** to save your changes.

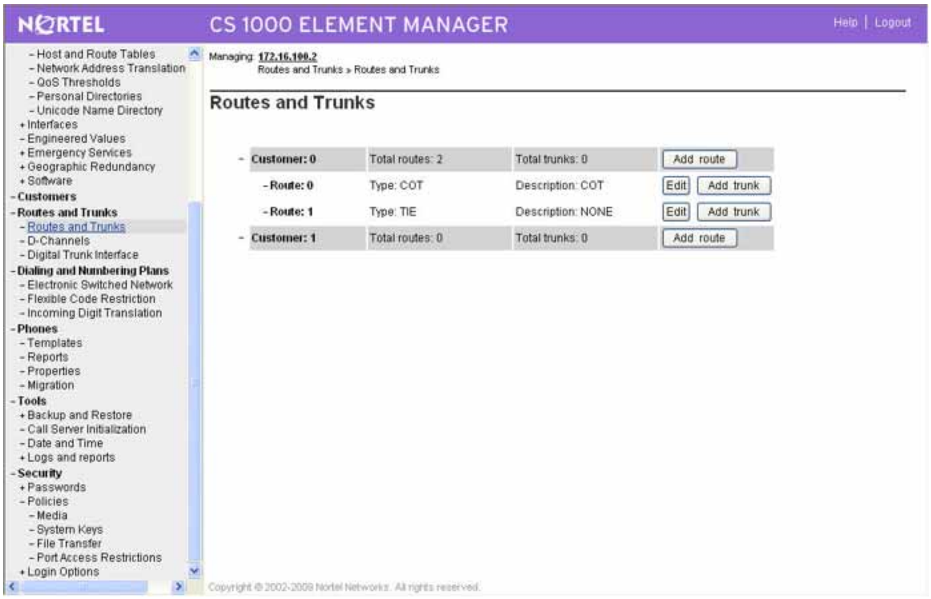
--End--

VTRK Class of Service configuration

You can configure Media Security Class of Service for Virtual Trunks (trunks that have XTRK configured as VTRK).

Procedure 53
Configuring VTRK Class of Service using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Routes and Trunks > Routes and Trunks**, and select a customer record.



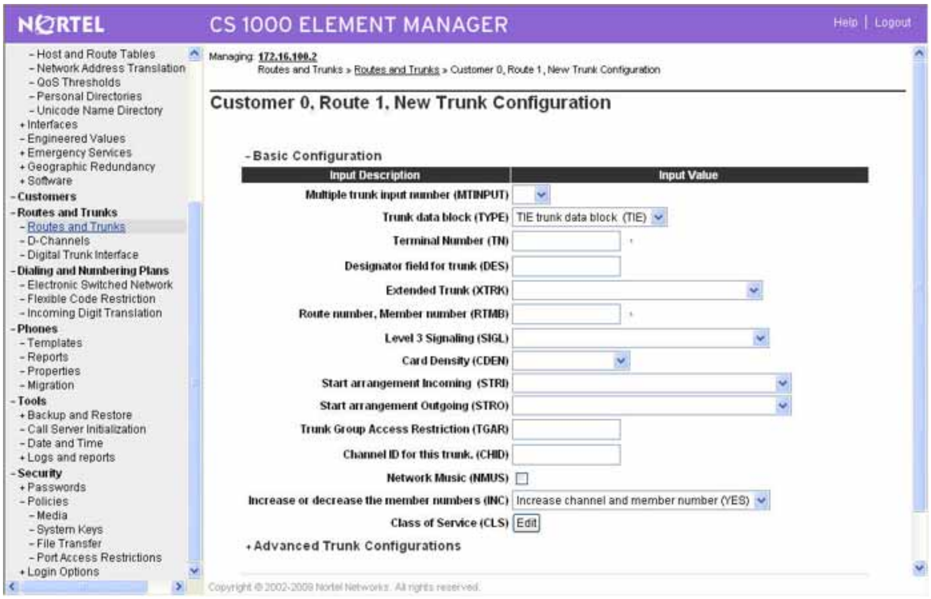
Managing: 172.16.100.2
Routes and Trunks » Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 0	Add route
- Route: 0	Type: COT	Description: COT	Edit Add trunk
- Route: 1	Type: TIE	Description: NONE	Edit Add trunk
- Customer: 1	Total routes: 0	Total trunks: 0	Add route

Copyright © 2002-2009 Nortel Networks. All rights reserved.

3	Click **Add Trunk** for the route to which you want to add a trunk. The New Trunk Configuration page appears.



Managing: 172.16.100.2
Routes and Trunks » Routes and Trunks » Customer 0, Route 1, New Trunk Configuration

Customer 0, Route 1, New Trunk Configuration

- Basic Configuration

Input Description	Input Value
Multiple trunk input number (MTINPUT)	
Trunk data block (TYPE)	TIE trunk data block (TIE)
Terminal Number (TN)	
Designator field for trunk (DES)	
Extended Trunk (XTRK)	
Route number, Member number (RTMB)	
Level 3 Signaling (SIGL)	
Card Density (CDEN)	
Start arrangement Incoming (STRI)	
Start arrangement Outgoing (STRO)	
Trunk Group Access Restriction (TGAR)	
Channel ID for this trunk. (CHID)	
Network Music (NMUS)	□
Increase or decrease the member numbers (INC)	Increase channel and member number (YES)
Class of Service (CLS)	Edit

+ Advanced Trunk Configurations

Copyright © 2002-2009 Nortel Networks. All rights reserved.

4 From the **Trunk datablock type** menu, select **IP Trunk (IPT1)**.

5 Enter the terminal number of the trunk in the **Terminal Number (TN)** field.

6 Ensure that the **Extended Trunk (XTRK)** field contains a value of **VTRK**.

7 Enter the RTMB in the **Route number, Member number (RTMB)** field.

8 Click **Edit** next to **Class of Service (CLS)**.

9 In the **Media Security (CLS)** menu, select one of the following Class of Service values:

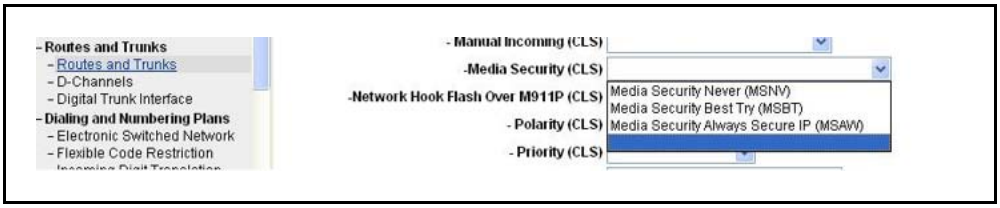
`MSNV` to configure the IP Phone Media Security Class of Service to Never, which disables Media Security on the IP Phone. The system does not attempt to secure either incoming or outgoing calls.

OR

`MSBT` to configure the IP Phone Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls.

OR

`MSAW` to configure the IP Phone Media Security Class of Service to Media Security Always Secure IP.


- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Manual Incoming (CLS)
-Media Security (CLS)
-Network Hook Flash Over M911P (CLS)
- Polarity (CLS)
- Priority (CLS)
Media Security Never (MSNV)
Media Security Best Try (MSBT)
Media Security Always Secure IP (MSAW)

10 Click **Return Class of Service**.

11 Click **Save**.

--End--

Media Security configuration using overlays

Use the procedures in this section to configure the Media Security feature using LD 11, 14, and 17.

System-wide Media Security configuration

You can configure a system-wide configuration setting that controls whether or not the Communication Server 1000 system provides Media Security. By default, Media Security is enabled on the system.

You can configure system-wide Media Security settings using LD 17. For more information about LD 17, see *Software Input Output Administration* (NN43001-611).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 54
Configuring system-wide Media Security using LD 17

Step **Action**

1 Log on to the Call Server CLI using a PWD2 account.

2 Enter **`CHG`** at the LD 17 `REQ` prompt.

3 Enter **`PARM`** at the LD 17 `TYPE` prompt.

4 Enter either the following commands at the LD 17 `MSEC` prompt:

`ON` to enable the Media Security feature at the system wide level for the Call Server. If you configure MSEC to ON, then IP Phones with a Class of Service other than MSNV can secure calls using Media Security, as can Mindspeed DSPs.

OR

`OFF` to disable the Media Security feature. When this option is selected, Media Security Class of Service settings on the IP Phones have no effect.

The default value for MSEC is ON.

5 Enter one of the following commands at the LD 17 `MSSD` prompt:

`MSNV` to configure the system-wide default value to Never, which disables Media Security on all IP Phones that have the security Class of Service configured as MSSD.

OR

`MSBT` to configure the system-wide default value to Best Effort, which configures Media Security to use Best Effort on all TNs that have the security Class of Service configured as MSSD.

OR

`MSAW` to configure the system-wide default value to Always, which configures Media Security to allow secure media exchanges only. Unsecured connection attempts are blocked.

The default value for MSSD is MSNV.

6 Enter **`<NKEY>`** at the LD 17 `NKEY` prompt.

7 Enter **`<TKEY>`** at the LD 17 `TKEY` prompt.

--End--

Table 34
Variable definitions

Variable	Value
<NKEY>	An integer in the range of 16-31. The default value for <NKEY> is 31, providing 2^{31} packets. The maximum number of packets that can be secured by a master key before it must be regenerated is calculated using the formula: number of packets = 2^{n}.
<TKEY>	An integer in the range of 8-168. This value is the maximum length of time, measured in hours, that a session key can remain valid. The default value for TKEY is 24 hours.

Class of Service configuration

Use LD 11 to assign a Media Security Class of Service for IP Phones. For more information about LD 11, see *Software Input Output Administration* (NN43001-611).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 55
Configuring Class of Service using LD 11

Step	Action
1	Log on to the Call Server CLI using a PWD2 account.
2	Enter **`CHG`** at the LD 11 `REQ` prompt.
3	Enter the IP Phone type at the LD 11 `TYPE` prompt. For example, **`2002p2`**, **`2050pc`**, or**`2004p2`**. This option is applicable to IP Line devices only. For any other type, entering a Media Security Class of Service value causes an error.
4	Enter the TN of a configured IP Phone of the type you selected in the previous step.
5	Enter **`YES`** at the LD 11 `ECHG` prompt.
6	Enter one of the following commands at the LD 11 `ITEM` prompt: **`CLS MSNV`** to configure the IP Phone Media Security Class of Service to Never, which disables Media Security on the IP Phone. The system does not attempt to secure either incoming or outgoing calls. **OR** **`CLS MSBT`** to configure the IP Phone Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls. **OR** **`CLS MSAW`** to configure the IP Phone Media Security Class of Service to Always. The system attempts to secure both incoming and outgoing calls; if the effort fails, the call is disconnected. **OR** **`CLS MSSD`** to configure the IP Phone Media Security Class of Service to use the system default. The default value for Class of Service is MSNV.
7	Press **Enter** until an REQ prompt appears.

--End--

For any of the Media Security parameters in LD 11 to take effect, you must turn on the system-wide Media Security option in LD 17, as described in "Media Security configuration using overlays" (page 201). When the Class of Service of an IP Phone is configured to CLS MSSD, the Class of Service for that IP Phone is dynamically configured to either MSNV or MSBT, depending on the configuration of the MSSD parameter in LD 17.

VTRK Class of Service configuration

You can configure Media Security Class of Service for Virtual Trunks (trunks that have XTRK configured as VTRK). Use LD 14 to configure Media Security Class of Service for Virtual Trunks. For more information about LD 14, see *Software Input Output Administration* (NN43001-611).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 56
Configuring VTRK Class of Service using LD 14

Step	Action
1	Log on to the Call Server CLI using a PWD2 account.

2	Enter one of the following commands at the LD 14 `REQ` prompt:
	`NEW`
	OR
	`CHG`

3	At the LD 14 `TYPE` prompt, enter **`IPTI`**. Entering any other TYPE value causes an error.
4	At the LD 14 `TN` prompt, enter **`<lscu>`**.
5	At the LD 14 `XTRK` prompt, press **Enter** to accept the value **`VTRK`**.
6	At the LD 14 `CUST` prompt, enter **`<customer num>`**.
7	At the LD 14 `RTMB` prompt, enter **`xy`**.
8	At the LD 14 `CHID` prompt, enter **`x`**.
9	At the LD 14 `STRI` prompt, enter **`IMM`**.
10	At the LD 14 `STRO` prompt, enter **`IMM`**.
11	At the LD 14 `CLS` prompt, enter either: **`MSNV`** to configure the VTRK Media Security Class of Service to Never, which disables Media Security on the IP Phone. The system does not attempt to secure either incoming or outgoing calls. **OR** **`MSBT`** to configure the VTRK Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls.

12 Press **Enter** at each subsequent prompt.

--End--

Table 35
Variable definitions

Variable	Value
<lscu>	Loop Shelf Card Unit value.
<customer num>	The customer number.

Media Security configuration information

Use the procedures in this section to access information about the configuration of the Media Security feature using overlays or from an IP Phone. For information about Media Security configuration using the Element Manager interface, see “Media Security configuration using Element Manager” (page 196).

Media Security configuration information available using overlays

This section provides information about tools you can use to access configuration information for Media Security from the command line interface (CLI).

Use the following procedure to view information about Media Security using LD 117.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 57
Viewing Media Security Settings using LD 117

Step **Action**

1 Log on to the Call Server CLI using a PWD2 account.

2 At the LD 117 prompt, enter **`PRT MSEC [ SYS | IP <ip_address> | TN <tn> | ALL ]`**.

For more information about the arguments for this command, see Table 36 "Job aid: commands to access information about Media Security configuration" (page 206).

--End--

Table 36
Job aid: commands to access information about Media Security configuration

Prompt	Response	Description
=>	PRT MSEC SYS	Prints the system-wide Media Security configuration. Prints if Media Security debug mode is enabled or disabled. Prints the remaining timeout value when the system automatically disables Media Security debug mode.
=>	PRT MSEC IP <ip_address>	Prints the Media Security Class of Service for a specified IP address. Prints if Media Security debug mode is enabled or disabled for the individual IP addresses and prints the remaining timeout values when Media Security debug mode for the IP addresses are automatically disabled. An IP address can be complete or partial. For example, PRT MSEC IP 47.11.0.0 prints the Media Security Class of Service for the IP Phones whose IP addresses are in the range from 47.11.0.0 to 47.11.255.255.
=>	PRT MSEC TN <tn>	Prints the Media Security Class of Service for a specified TN. Prints if Media Security debug mode is enabled or disabled for the individual terminals and prints the remaining timeout values when Media Security debug mode for the terminals are automatically disabled. A TN can be complete or partial. For example, PRT MSEC TN 61 prints the Media Security Class of Service for IP Phones whose TNs are in the range from (61, 0) to (61, maximum).
=>	PRT MSEC ALL	Prints the system-wide Media Security configuration, as well as the Media Security Class of Service for all TNs. Prints if Media Security debug mode is enabled or disabled. Prints the remaining timeout value when the system automatically disable Media Security debug mode. Prints if Media Security debug mode is enabled or disabled for the individual terminals and prints the remaining timeout values when Media Security debug mode for terminals are automatically disabled.

Use the following procedure to view information about system-wide Media Security settings using LD 22.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 58
Viewing system-wide Media Security settings using LD 22

Step	Action
1	Log on to the Call Server CLI using a PWD2 account.
2	At the LD 22 `REQ` prompt, enter **`PRT`**.
3	At the LD 22 `TYPE` prompt, enter **`PARM`**.

--End--

Use the following procedure to view information about user level Class of Service using LD 11 or LD 20.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 59
Viewing user level Class of Service settings using LD 11 or LD 20

Step	Action
1	Log on to the Call Server CLI using a PWD2 account.
2	At the LD 20 or LD 11 `REQ` prompt, enter **`PRT`**.
3	At the LD 20 or LD 11 `TYPE` prompt, enter **`TNB`**.
4	At the LD 20 or LD 11 `TN` prompt, enter **`<lscu>`**.
5	Press **Enter** at each subsequent prompt.

--End--

Table 37
Variable definitions

Variable	Value
<lscu>	Loop Shelf Card Unit value.

Media Security information available using an IP Phone

Use the following procedure to view the Media Security configuration of an IP Phone using the menus on the IP Phone.

Procedure 60
Viewing Media Security information using an IP Phone

Step	Action
1	On an IP Phone, open the **Telephone Options** menu.
2	Use the navigation keys to scroll and select **Set Info**, and press the **Send/Enter** key.
3	Use the navigation keys to scroll and select **Encryption Info**, and press the **Send/Enter** key.
4	Use the navigation keys to scroll and view **Encryption Capability** or **Encryption Policy**. For more information about the information shown, see "Class of Service configuration" (page 202).
5	Press the **Cancel** soft key to return to the main menu.

--End--

SIP Route information available using overlays

Use the following procedure to view SIP Route information by using LD 21.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 61
Viewing SIP Route information by using LD 21

Step	Action
1	At the LD 21 `REQ` prompt, enter **`PRT`**.
2	At the LD 21 `TYPE` prompt, enter **`RDB`**.
3	At the LD 21 `CUST` prompt, enter **`<customer number>`**.
4	At the LD 21 `ROUT` prompt, enter **`<route number>`**.

--End--

User and password management

This chapter contains procedures to help you manage users, passwords, and privileges. The chapter is divided into the following sections:

- “Account types and roles” (page 212)
- “User and password management using overlays” (page 214)
- “User and password management using Element Manager” (page 234)

ATTENTION
Backup and restore operations for Linux-based UCM elements involve critical data that can have possible impacts to system security. You should consider data security and accountability when assigning roles and permissions for user accounts that have backup and restore privileges. To ensure optimum security of backup data for Linux base elements Nortel recommends using the central backup and restore common service through the UCM primary server Deployment Manager, for backup and restore operations of all Linux based UCM member elements.

For maintenance procedures that require the system operator to invoke backup and restore operations locally from the Linux base UCM member element, Nortel recommends using a securely managed external sFTP server. Security auditing procedures should be implemented to verify compliance by system operators.

System operators should avoid the routine use of Linux Base Manager or Linux CLI commands to backup the Linux base UCM member element to a local removable storage device

For more information about user and password management concepts on Communication Server 1000, see “User and password management concepts” (page 45).

For information about configuring users using Unified Communications Management, see *Unified Communications Management Fundamentals* (NN43001-116).

> ***Note:*** After upgrading to Communication Server Release 6.0, all user accounts created in previous releases must be recreated using Unified Communications Management in order for them to be recognized by Radius.For VxWorks-based elements (except Call Servers), the accounts database is reset to default during the upgrade. After the upgrade, only the default accounts are in service until the element joins the UCM secure domain, at which time it receives the updated accounts database file from the Call Servers.

Roles and permissions

In Communication Server 1000 Release 6.0, IP telephony systems must use UCM central authentication to manage system level OAM and PDT users and passwords. UCM features both built-in and custom 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.

You can map custom roles 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, you must create custom roles 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.

For information about UCM built-in and custom roles, see *Unified Communications Management Fundamentals* (NN43001-116).

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 (e.g. 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.

For information about role inheritance and permission mapping, see *Unified Communications Management Fundamentals* (NN43001-116).

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 CS 1000, 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 information about permission templates, see *Unified Communications Management Fundamentals* (NN43001-116).

Account types and roles

Each user has one of the following account types:

- PWD2 provides OAM level access that includes system security, account administration and general system administration
- PWD1 provides OAM level access that includes general system administration
- LAPW provides OAM level access that is restricted to user specified administration operations
- PDT1 provides PDT level access for expert technicians and Nortel Support group
- PDT2 provides ROOT level access for Nortel Developers

In addition to the access privileges and limitations that each account type offers, you can assign specific privileges to each user.

This chapter provides procedures to help you manage users and configure user privileges.

Account synchronization

When you add a user or change a password, the system automatically schedules an Equipment Data Dump (EDD) to update the accounts on each local device. When an EDD occurs, the system distributes the updated account files to all Voice Gateway Media Card, Media Gateway Controller (MGC), and IP Media Gateway (IPMG) devices. The EDD normally runs at the next virtual midnight, so changes can take up to 24 hours to be propagated to all parts of the system. To force an immediate EDD, see “Force an EDD using overlays” (page 301).

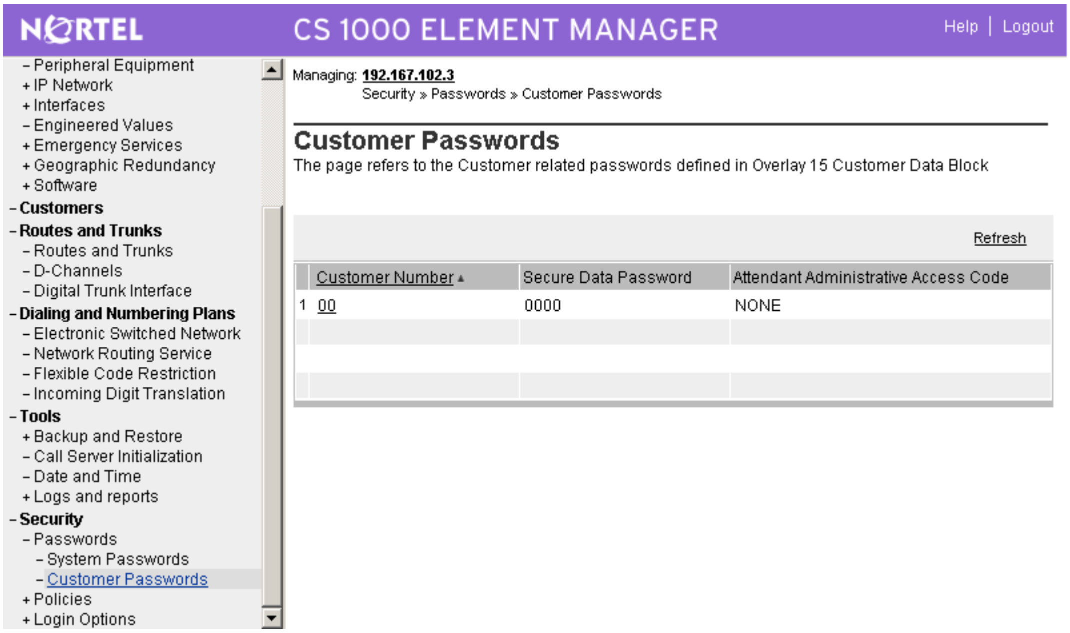
Customer passwords

For each Customer Number defined on the system, you can assign a Secure Data Password and an Attendant Administrative Access Code.

Use the following procedure to assign or change the Secure Data Password or Attendant Administrative Access Code.

Procedure 62
Assigning or changing customer passwords

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Passwords > Customer Passwords** . The **Customer Passwords** page appears.



Managing: **192.167.102.3**
Security » Passwords » Customer Passwords

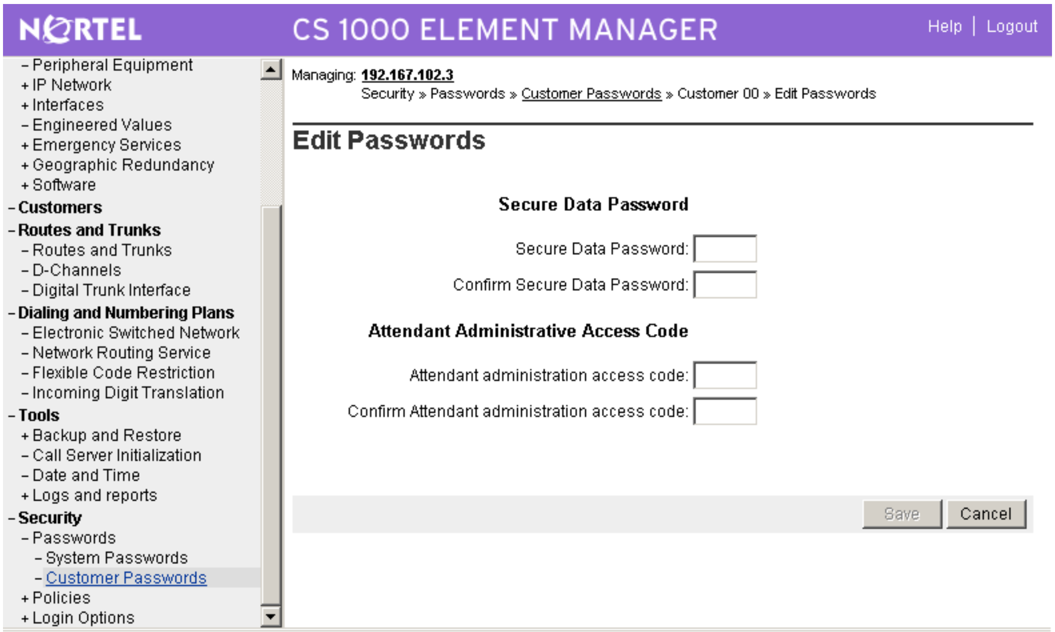
Customer Passwords

The page refers to the Customer related passwords defined in Overlay 15 Customer Data Block

	Customer Number ▲	Secure Data Password	Attendant Administrative Access Code
1	00	0000	NONE

3 Click a Customer Number.

The **Edit Passwords** page appears.



Managing: **192.167.102.3**
Security » Passwords » Customer Passwords » Customer 00 » Edit Passwords

Edit Passwords

Secure Data Password

Secure Data Password:

Confirm Secure Data Password:

Attendant Administrative Access Code

Attendant administration access code:

Confirm Attendant administration access code:

4 Type the new secure data password in the **Secure Data Password**: field, and in the **Confirm Secure Data Password**: field.

5 Type the new secure data password in the **Attendant administration access code**: field, and in the **Confirm Attendant administration access code**: field.

6 Click **Save**.

The **Customer Passwords** page appears.

--End--

User and password management using overlays

Use the information in this section to manage users, passwords, and privileges using LD 17 and LD 22.

User management

Use the procedures in this section to create, configure, and delete users.

Add a user

Use the following procedure to add a new PWD1 or PWD2 user.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 63
Adding a user other than LAPW by using LD 17

Step Action

1 Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.

2 At the LD 17 `REQ` prompt, enter **`CHG`**.

3 At the LD 17 `CHG` prompt, enter **`PWD`**.

4 Bypass subsequent prompts (that deal with password settings, described later in this chapter) by pressing **Enter** at each one, until you reach the `ACCOUNT_REQ` prompt.

5 At the `ACCOUNT_REQ` prompt, enter **`NEW`** to create a new user.

6 At the `PWD_TYPE` prompt, enter **`<account type>`**.

7 At the LD 17 `USER_NAME` prompt, enter the user name to add or edit.

8 At the LD 17 `PASSWORD` prompt, enter the new password for the user, and reenter it at the `CONFIRM` prompt.

9 For PWD2 users, at the LD 17 `ACCT` prompt, enter either:

`YES` to enable account management privileges for the new user,

OR

NO to disable account management privileges for the new user.

10 At the LD 17 PDT prompt, enter either:
PDT1 to grant the user access to PDT level one,

OR

PDT2 to grant the user access to PDT level two.

--End--

Table 38
Variable definitions

Variable	Value
<account type>	The type of account to create.

Table 39
Job aid: Restrictions on LAPW user names and passwords

Each LAPW user name can be up to 11 alphanumeric characters.
For LAPW SBA type users, the password must be 4-16 nonsequential numeric characters, and must consist of the digits 0-9 only.

The sequence of prompts for LD 17 is shown in Table 40 "Job aid: LD 17 user and password prompts" (page 215).

Table 40
Job aid: LD 17 user and password prompts

Prompt	Response	Comment
REQ:	CHG	Change.
TYPE:	PWD	Configuration Record.
PSWD_COMP	(OFF) ON	Turns on or off the password complexity check for the ADMIN, LAPW and PDT passwords.
FPC	(NO) YES	Force Password Change.
LOUT	1–(20) – 1440	Logout, Inactive Session Logout Time in minutes.
FLTH	0–(3)–9	Failed Log In Threshold.
LOCK	0–(60)–270	Lockout time.
FLTA	(NO) YES	Failed Log In Threshold Alarm.
AUDT	(NO) YES	Audit Trail for password usage.
- SIZE	(50)-1500	Word Size of Audit Trail buffer.

Table 40
Job aid: LD 17 user and password prompts (cont'd.)

LLID	(NO) YES	Last Log In Identification.
ACCOUNT_REQ	aaa	Account Request, where: aaa = (END), NEW, CHG, or OUT.
PWD_TYPE	aaa	Specifies the user type being added to the system, where: aaa = PWD2, PWD1, LAPW.
- PWTP	(OVLY) SBA	Type of LAPW account: (OVLY) Overlay Password Access Type (SBA) Set-Based Administration Password Access Type.
USER_NAME	a...a	Unique user name — up to 11 characters.
PASSWORD	a...a	Password associated with the user name entered at the USER_NAME prompt. For password requirements, see Table 48 "Job aid: Password restrictions" (page 227).
NEW_PASSWORD	a...a	New password. For password requirements, see Table 48 "Job aid: Password restrictions" (page 227).
CONFIRM	a...a	Confirm the new password
ACCT	(NO) YES	Administer accounts. This prompt appears only when you add or modify Level 2 (PWD2) users.
PDT	(NO) PDT1, PDT2	PDT Access. This prompt appears only when you add or modify LAPW, Level 1 (PWD1) and Level 2 (PWD2) users.
OVLA	xx xx ... xx	Overlays Allowed
LEVL	aaaa	Access Level for Set Based Administration password, where; aaaa = (INST) or ADMN
CUST	aaa	Customer to be accessible by way of PWnn
TEN	xx	Tenant number (1–151)
HOST	(NO) YES	Enable HOST mode Log In for password PWnn
MAT	(NO) YES	Enable MAT Log In for password PWnn
OPT	a...a	Options for password PWnn
PDT	xxxx	PDT1 or PDT2

Note: For more information about the prompts and responses in LD 17, see *Software Input Output Administration* (NN43001-611).

Add an LAPW user

Use the Limited Access to Overlays feature to create Limited Access Passwords (LAPW). LAPW users can access only the overlays you specify. You can define LAPW users that have regular access to specific overlays or that have Print Only capability, and you can use LAPW Audit Trail to track access to the system by LAPW users. The LAPW Audit Trail stores logon time, name, and password, and provides a time stamp indicating when the user logged out.

Use the procedures in this section to add and configure LAPW users. For more information about the prompts and options in LD 17, see *Software Input Output Administration* (NN43001-611).

Use the following procedures to create an LAPW user with Limited Access to Overlays type access:

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 64
Adding an LAPW (Overlay) user by using LD 17

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 17 `REQ` prompt, enter **`CHG`**.
3	At the LD 17 `TYPE` prompt, enter **`PWD`**.
4	Bypass subsequent prompts by pressing **Enter** at each one.
5	At the LD 17 `ACCOUNT_REQ` prompt, enter **`NEW`** to add a new user.
6	At the LD 17 `PWD_TYPE` prompt, enter **`LAPW`**.
7	At the LD 17 `PWTP` prompt, enter **`OVLY`** to create an LAPW user that has Overlay Password Access.
8	At the LD 17 `USER_NAME` prompt, enter the user name to add or edit. SeeTable 43 "Job aid: Restrictions on LAPW user names and passwords" (page 220) for information about the restrictions on LAPW user names.
9	At the LD 17 `PASSWORD` prompt, enter the new password for the user, and reenter it at the `CONFIRM` prompt. SeeTable 48 "Job aid: Password restrictions" (page 227) for information about the restrictions on passwords.
10	At the LD 17 `OVLA` prompt, enter the overlays the new user can access.
11	At the LD 17 `CUST` prompt: press **Enter** to give the user access to all customer records, **OR**

enter **<customer num>** , and then enter **TEN <tenant num>**, to specify the customers the user can access.

12 At the LD 17 `HOST` prompt, enter either:
YES to enable HOST mode Log On for password PWnn,
OR
NO to disable HOST mode Log On for password PWnn.

13 At the LD 17 `MAT` prompt, enter either:
YES to enable MAT Log On for password PWnn,
OR
NO to disable MAT Log On for password PWnn.
If this option is enabled, MAT 5.0 users can remotely log on and perform Alarm Management and Maintenance operations through a graphical interface.

14 At the LD 17 `MAT_READ_ONLY` prompt, enter **YES** to grant MAT write access for password PWnn,
OR
NO to deny MAT write access for password PWnn.
Read-only users cannot clear or acknowledge alarms, and can use status commands only.

15 At the LD 17 `OPT` prompt, enter **<options>**.

16 At the LD 17 `PDT` prompt, enter either:**PDT1** to grant the user access to PDT level one,
OR
PDT2 to grant the user access to PDT level two.

--End--

Table 41
Variable definitions

Variable	Value
<customer num>	The customer number.
<options>	The password options permitted for password PWnn.
<tenant num>	The tenant number.

Use the following procedure to create an LAPW user with Set Based Administration access:

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 65
Adding an LAPW (Set Based Administration) user by using LD 17

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 17 `REQ` prompt, enter **`CHG`**.
3	At the LD 17 `TYPE` prompt, enter **`PWD`**.
4	Bypass subsequent prompts by pressing **Enter** at each one.
5	At the LD 17 `ACCOUNT_REQ` prompt, enter **`NEW`** to add a new user.
6	At the LD 17 `PWD_TYPE` prompt, enter **`LAPW`**.
7	At the LD 17 `PWTP` prompt, enter **`SBA`** to create an LAPW user that has Set Based Access.
8	At the LD 17 `USER_NAME` prompt, enter the user name to add or edit. See Table 43 "Job aid: Restrictions on LAPW user names and passwords" (page 220) for information about the restrictions on LAPW user names.
9	At the LD 17 `PASSWORD` prompt, enter the new password for the user, and reenter it at the `CONFIRM` prompt. For LAPW SBA type users, the password must be 4-16 numeric characters, and must consist of the digits 0-9 only.
10	At the LD 17 `LEVL` prompt, enter either: **`INST`** to configure the access level of the user to be Installer, **OR** **`ADMN`** to configure the access level of the user to be Administrator.
11	At the LD 17 `CUST` prompt: press **Enter** to give the user access to all customer records, **OR** enter **`<customer num>`** , and then enter **`TEN <tenant num>`**, to specify the customers the user can access.
12	At the LD 17 `OPT` prompt, enter **`<options>`**.

--End--

Table 42
Variable definitions

Variable	Value
<customer num>	The customer number.

Table 42
Variable definitions (cont'd.)

<options>	The password options permitted for password PWnn.
<tenant num>	The tenant number.

For more information about the password options that you can enter at the OPT prompt, see *Software Input Output Administration* (NN43001-611).

Table 43
Job aid: Restrictions on LAPW user names and passwords

Each LAPW user name can be up to 11 alphanumeric characters.
For LAPW SBA type users, the password must be 4-16 nonsequential numeric characters, and must consist of the digits 0-9 only.

For more information about LAPW and the prompts in LD 17 and LD 22, see *Software Input Output Administration* (NN43001-611).

View all user accounts

Use the following procedure to display detailed information about all user accounts. Passwords are not displayed.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 66
Viewing account information by using LD 22

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 22 `REQ` prompt, enter **`prt`**.
3	At the LD 22 `TYPE` prompt, enter **`pwd`**. Details of all accounts appear.

--End--

Table 44 "Example output from the PRT PWD command" (page 221) shows an example of the output from the PRT PWD command.

Table 44
Example output from the PRT PWD command

```
PWD
PSWD_COMP ON
LOUT 20
FLTH 3
LOCK 30
FLTA NO
AUDT NO
LLID NO
INIT NO
USER_NAME NORTEL2 **INSECURE**
TYPE PWD2
USER_NAME NORTEL1 **INSECURE**
TYPE PWD1
USER_NAME LAPW1 **INSECURE**
TYPE LAPW)
OVLA   001   002   003   004   005   006   007   008   009   010
       011   012   013   014   015   016   017   018   019   020
       021   022   023   024   025   026   027   028   029   030
       031   032   033   034   035   036   037   038   039   040
       041   042   043   044   045   046   047   048   049   050
       051   052   053   054   055   056   057   058   029   060
       061   062   063   064   065   066   067   068   069   070
       071   073   073   074   075   076   077   078   079   080
       081   082   083   084   085   086   087   088   089   090
       091   092   093   094   095   096   097   098   099   117
       135   137   143
CUST
HOST NO
MAT NO
OPT PSCA RBBD CFPA LLCD PROD LOSD FORCD MOND
USER_NAME LAPW3 **INSECURE**
TYPE LAPW_OVL
OVLA 017 022
CUST
HOST NO
MAT NO
OPT PSCA RDBD DFPA LLCD PROD LOSE FORCD MOND
USER_NAME SBA2
PWTP SBA
LEVL ADMN
CUST
OPT FEAD NAMA TADD TOLD DTD TRKD INSD
```

Check for Insecure passwords

Use the following procedure to display detailed information about user that have insecure passwords. Passwords are not displayed.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 67
Checking for insecure passwords using LD 22

Step	Action
1	At the LD 22 `REQ` prompt, enter **`PRT`**.
2	At the LD 22 `TYPE` prompt, enter **`IPWD`**.

--End--

Table 45 "IPWD output" (page 222) shows an example of the output form the PRT IPWD command.

Table 45
IPWD output

```
PWD
User_Name NORTEL2 **INSECURE**
TYPE PWD2
User_Name NORTEL1 **INSECURE**
TYPE PWD1
USER_NAME LAPW1 **INSECURE**
TYPE LAPW_OVL
USER_NAME LAP3 **EXPIRED**
TYPE LAPW3_OVL
```

Configure LAPW Audit Trail using overlays

The Audit Trail for Limited Access Password (LAPW) stores logon time, name, and password, and includes time stamps that indicate when users logged out.

Use the following procedure to enable or disable Audit Trail and configure the size of the Audit Trail file.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 68
Configuring the LAPW Audit Trail by using LD 17

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 17 `REQ` prompt, enter **`CHG`**.
3	At the LD 17 `TYPE` prompt, enter **`PWD`**. You can bypass any of the subsequent prompts by pressing **Enter**. For more information about the sequence of prompts for LD 17, see Table 40 "Job aid: LD 17 user and password prompts" (page 215).
4	At the LD 17 `AUDT` prompt, enter either: **`YES`** to enable the Audit Trail, **OR** **`NO`** to disable the Audit Trail.
5	At the LD 17 `SIZE` prompt, enter **`<SIZE>`**. After the Audit Trail file becomes full, no more information can be stored in it. Nortel recommends periodically backing up the file and deleting the contents.
6	Bypass subsequent prompts by pressing **Enter** at each one.

--End--

Table 46
Variable definitions

Variable	Value
<SIZE>	The word size for the Audit Trail file, in the range of 50–1500. The default value is 50.

Use the following procedure to access information stored in the Audit Trail.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 69
Viewing information stored in the LAPW Audit Trail by using LD 22

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 22 `REQ` prompt, enter **`PRT`**.

3 At the LD 22 `TYPE` prompt, enter **`AUDT`** to view the Audit Trail.

--End--

Delete a user

Use the following procedure to remove a user.

Procedure 70
Deleting a user by using LD 17

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 17 `REQ` prompt, enter **`CHG`**.
3	At the LD 17 `CHG` prompt, enter **`PWD`**.
4	Bypass subsequent prompts by pressing **Enter** at each one, until you reach the `ACCOUNT_REQ` prompt.
5	At the `ACCOUNT_REQ` prompt, enter **`OUT`** to delete a user.
6	At the `USER_NAME` prompt, enter the name of the user to delete. The following message appears: `WARNING: THIS ACCOUNT WILL BE DELETED OK? (Y/N)`
7	Enter **`Y`** to delete the user.

--End--

Password management

Use the information in this section to change passwords and view information about user accounts. The sequence of prompts for LD 17 is shown in Table 40 "Job aid: LD 17 user and password prompts" (page 215).

To view LAPW prompts, you must equip package 164 LAPW Limited Access to Overlays. LAPW users can change their passwords by entering the current password at prompt LPWD and entering the new password at the NLPW prompt.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 71
Changing a password by using LD 17

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2	At the LD 17 `REQ` prompt, enter **`CHG`**.
3	At the LD 17 `CHG` prompt, enter **`PWD`**.
4	Bypass subsequent prompts by pressing **Enter** at each one.
5	At the `ACCOUNT_REQ` prompt, enter **`CHG`**.
6	At the `USER_NAME` prompt, enter the user name to change the password.
7	At the `NEW_PASSWORD` prompt, enter the new password, and reenter it at the `CONFIRM` prompt.

--End--

You can use the following procedure to change the password for your PDT user name using the PDT shell command line interface (CLI).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 72
Changing your PDT password by using the CLI

Step	Action
1	Log on to the Call Server CLI using an account that has PDT privilege.
2	Access the PDT prompt by holding down the **`ctrl`** key, and typing **`pdt`**. The PDT prompt appears.
3	Enter the command **`passwd`**.
4	Enter your existing password.
5	Enter the new password. The new password must be different from the current password.
6	Reenter the new password. A confirmation message appears.

7 To exit PDT mode, type **`exit`**, and press **Enter** twice.

--End--

These changes are distributed to all Voice Gateway Media Card, MGC, and IPMG devices the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see "Force an EDD using overlays" (page 301).

Global password settings configuration

Use the procedure in this section to implement password settings that apply to all accounts. For more information about the features implemented in this procedure, see "Global password settings" (page 48). For recommendations about what password settings to use, see "Recommended password management practices" (page 52).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

> **ATTENTION**
> Nortel recommends that you change the default passwords. The Default Password Change feature improves the security of a system by providing a default system password warning message and a Force Password Change (FPC) prompt.

Procedure 73
Configuring password settings by using LD 17

Step Action

1 Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.

2 At the LD 17 `REQ` prompt, enter **`CHG`**.

3 At the LD 17 `CHG` prompt, enter **`PWD`**.

You can bypass any of the following prompts by pressing **Enter**. For more information about the sequence of prompts for LD 17, see Table 40 "Job aid: LD 17 user and password prompts" (page 215).

4 At the LD 17 `PSWD_COMP` prompt, enter **`ON`** to enable Password Complexity Checking for ADMIN, LAPW, and PDT users.

For more information about password complexity restrictions, see Table 48 "Job aid: Password restrictions" (page 227).

5 At the LD 17 `FPC` prompt, enter **`YES`** to enable Force Password Change.
Configuring FPC to YES closes LD 17; to continue configuring

password settings in LD 17, repeat steps 2-4, enter NO at the FPC prompt, and then proceed to step 6.

The FPC = YES value is not retained in the database and must be configured to YES each time you want to force a change.

6 At the LD 17 `LOUT` prompt, enter **`<LOUT>`** to enable Inactive Session Timeout.

7 At the LD 17 `FLTH` prompt, enter **`<FLTH>`** to enable Failed Log in Threshold.

8 At the LD 17 `LOCK` prompt, enter **`<LOCK>`** to configure the Lockout time.

9 At the LD 17 `FLTA` prompt, enter **`YES`** to enable Failed Log In Threshold Alarm.

10 At the LD 17 `AUDT` prompt, enter **`YES`** to enable Audit Trail for password usage.
The `SIZE` prompt appears.

11 At the LD 17 `SIZE` prompt, enter **`<SIZE>`** to configure the word size of Audit Trail buffer.

12 At the LD 17 `LLID` prompt, enter **`YES`** to enable Last Login Identification.

13 Bypass subsequent prompts by pressing **Enter** at each one.

--End--

Table 47
Variable definitions

Variable	Value
<SIZE>	The word size for the Audit Trail file, in the range of 50–1500. The default value is 50.
<FLTH>	The number (in the range 0–9) of times a user can successively fail to log on before their account is locked out.
<LOCK>	The number (in the range 0–270) of minutes an account remains locked after the Failed Log in Threshold is reached.
<LOUT>	The number (in the range 1–1440) of minutes of inactivity before a session ends automatically.

Table 48
Job aid: Password restrictions

Password must be at least eight characters in length
The following characters are permitted: 0-9, A-Z, a-z, !$%^&()_- +={}|\:;"'<,>.?/

Table 48
Job aid: Password restrictions (cont'd.)

The following characters are not permitted: Spaces ~ ' * @ [ ] and #
Password must not: • contain the user name in forward or reverse order • have a keyboard trail • contain repeated strings • have four or more consecutive characters of the same type (lowercase alphabetic, uppercase alphabetic, and numeric) • have five or more consecutive alphabetic characters

Password reset

Use the procedures in this section to reset passwords on the Call Server, or on other devices. To use these procedures, you must disable UCM central authentication and reset the locally-authenticated Communication Server 1000 Call Server accounts (admin1, admin2, pdt2). You must have the applicable software install media (floppy disk or flash card) on hand, and must insert it only when prompted to do so during the password reset procedure.

Use the following procedure to reset an individual password on the Call Server, and lock out all other accounts. To protect against unauthorized use, Nortel has deliberately designed the password reset mechanism to require the user to be physically present in the switchroom to complete the procedure. The system also logs each attempt to reset a password. The system password reset procedure described in this section replaces all previously available methods of password override or password reset.

Procedure 74
Resetting Call Server passwords by using the CLI

Step	Action
1	Log on to the Call Server CLI using an account that has PDT privilege.
2	Access the PDT prompt by holding down the **`ctrl`** key, and typing **`pdt`**. The PDT prompt appears.

3	Instead of entering a user name, enter **`resetPWD`**.
	The Password Reset Mechanism is initiated, and the following message appears:
	`PDT login on /tyCo/0`
	`Username:  resetPWD`

```
************************************************
*
* WARNING: All attempts to use the Password Reset
Mechanism *
* are logged.  In order to proceed, you will need *
* physical access to the Call Server.  *
************************************************

If you do not wish to proceed, enter the word QUIT,
otherwise
enter the PWD2/Admin2 userID:
SEC026 Password override mechanism was used to gain
access to the switch
```

4. Enter either:
   `QUIT` to exit without resetting any passwords,
   OR
   `<user name>`.

   If the user name you enter exists on the system, it is the target of the password reset. If the user name you enter does not exist on the system, a new PWD2 level account is created.

5. When prompted, insert the install media in the disk drive or PC Card slot. You must complete this step within 60 seconds, or the Password Reset Mechanism cancels.

6. Press **Enter**.

7. Enter the new PWD2 password.

8. Reenter the new PWD2 password.

9. To exit PDT mode, type **`exit`**, and press **Enter** twice.

10. Remove the install media from the drive.

    The system changes the password for the account (or creates a new account and assigns it the new password) and locks out all other accounts. The system marks the new password as expired, so the user must change it on their next log on. If the account is locked because the user exceeded the Failed Log in Threshold, the system unlocks it.

    These changes are distributed the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see "Force an EDD using overlays" (page 301).

--End--

Table 49
Variable definitions

Variable	Value
<user name>	A PWD2 level user name.

Use the following procedure to reset the password on an MGC.

Procedure 75
Resetting MGC passwords by using the CLI

Step	Action

1 Use a direct serial connection to connect to the CLI of the MGC.

2 At the log on prompt, enter the reset password command:
`Username: resetPWD`.
The following output appears:

```
************************************************
*
* WARNING: All attempts to use the Password Reset
Mechanism *
* are logged.  In order to proceed, you will need *
* physical access to the Call Server.  *
************************************************
*
If you do not wish to proceed, enter the word QUIT,
otherwise
enter the PDW2/Admin2 userID:
```

3 Enter the user name for which you want to reset the password.
The following output appears:

```
You have 60 seconds to push the reset faceplate
button
```

4 Press the reset button on the MGC faceplate.
The following output appears:

```
You have 60 seconds to press ENTER:
```

5 Press **Enter**.
The following output appears:

```
Enter new password:  .
```

6 Enter the new password.
The following prompt appears:
`Reenter new password:`

7 Reenter the new password.

--End--

Password reset for other devices

For information about password reset procedures on other devices, see Table 50 "Password reset for Linux base elements" (page 231).

> **ATTENTION**
> To reset the password on MGC and Voice Gateway Media Cards, ensure that the card is properly registered to the Call Server and then reboot the card. This forces synchronization of the user names and passwords with the Call Server user names and passwords.

Table 50
Password reset for Linux base elements

Device or application	For more information about the reset procedure, see:
CallPilot mailbox	*CallPilot Manager Set Up and Operation Guide* (NN40090-300)
Contact center user	*Contact Center Manager Server Installation and Maintenance* (297-2183-925) and *Contact Center Manager Server Installation and Maintenance Guide for the Co-resident Server* (297-2183-925)
Hospitality Integrated Voice Services	*Hospitality Integrated Voice Services Fundamentals* (NN43001-559)
Integrated Call Director	*Nortel Integrated Call Director Service Implementation Fundamentals* (NN43001-561)
IP Line	*Signaling Server IP Line Applications Fundamentals* (NN43001-125)
Signaling Server	*Signaling Server IP Line Applications Fundamentals* (NN43001-125)

If Service Provider certificates are installed on an IP Phone, you can remove them by resetting the phone security policies, and other values, to factory defaults. For more information, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Multi-user login configuration using overlays

For normal system management access for multi-user login configurations, use Element Manager, UCM Central Deployment Manager and Patching Manager, and web services API in preference to using OAM CLI access.

Enable Multi-user login to permit up to five users to simultaneously log on to a system. Each user can load a different overlay (LD), and a sixth overlay (virtual midnight or background) can also run. If a user tries to load an overlay that another user is already using, an error message appears. This feature supports only:

- telephone administration
- maintenance

- midnight routines
- background routines
- attendant administration

Multi-user login supports a maximum of five users; if a sixth user attempts to log in, the system blocks the attempt. Use the monitor command to monitor the input/output activities on another local or remote terminal.

You can configure Multi-user login using LD 17, and view information about Multi-user login configuration using LD 22. For more information, see *System Management Reference* (NN43001-600).

Single Terminal Access configuration using overlays

Nortel does not recommend the use of the Single Terminal Access (STA) feature. If you want to provide remote access to multiple SDI ports on the Communication Server 1000 system elements and auxiliary servers and devices, Nortel recommends using an optional IP terminal server and to obtain technical support for configuring the terminal server from the terminal server equipment vendor.

uses Multipurpose Serial Data Link (MSDL), which reduces the number of physical devices you must have for administration and maintenance. For remote access over IP networks, you can configure a terminal server to provide a cost-effective method of switching between EIA232 serial port devices. When a user switches from one system to another, a mechanism for ending the original session is provided in the STA application through a configurable logoff sequence. This logoff sequence is specified in the database with each STA port, and is automatically sent to the destination system.

To protect against unauthorized access, the following rules apply:

- Users cannot leave the system without logging off, preventing users from leaving a session open in the background. If the logoff sequence is not configured correctly, the user can leave a program open in the background, which can lead to unauthorized access.
- If the modem connection is terminated, the STA master terminal uses the configured logoff sequences to automatically exit from the active and existing background sessions.
- A password is required before the user can enter **`NEW`** or **`CHANGE`** to configure an STA port. This process is designed to protect the STA port from unauthorized alteration.

You can configure STA using LD 17, and view information about STA configuration using LD 22. For more information, see *System Management Reference* (NN43001-600).

History File configuration using overlays

Use the History File to store system messages in memory. You can access or print the stored information using a system terminal or a remote device.

You can specify the types of information to be stored in the History File, including:

- maintenance messages (MTC)
- service change activity (SCH)
- customer service change activity (CSC)
- software error messages (BUG)

You can configure the History File using LD 17. For more information, see *System Management Reference* (NN43001-600).

Viewing the History File

You can selectively view the History File using the VHST command in LD 22, which offers the following options:

- search forward
- repeat the last search
- go up or down
- define the next or previous number of lines to display
- display lines from the current location to the bottom of the file
- search on a string of up to 12 characters

You can create a Traffic Log file that is separate from the History File.

You can view the History File using LD 22. For more information, see *System Management Reference* (NN43001-600).

Password management for stand-alone Signaling Server

Level 2 (PWD2) users can manage accounts and passwords on the stand-alone Signaling Server running Network Routing Service (NRS). Commands that you can issue from the OAM shell are shown in Table 51 "User administration commands" (page 234).

Table 51
User administration commands

Command	Description
adminUserPasswordChange [userID]	To change a password (any user can change their own password, but only users that have Level 2 [PWD2] privilege can change the password of another user). Where `userID` is the name of the user account to change.
adminUserCreate [userID]	To create an account (requires Level 2 (PWD2) privilege). Where `userID` is the name of the user account to create.
adminUserDelete [userID]	To delete an account (requires Level 2 (PWD2) privilege). Where `userID` is the name of the user account to delete.
adminAccountShow	To display all configured accounts on the system (requires Level 2 (PWD2) privilege).

User and password management using Element Manager

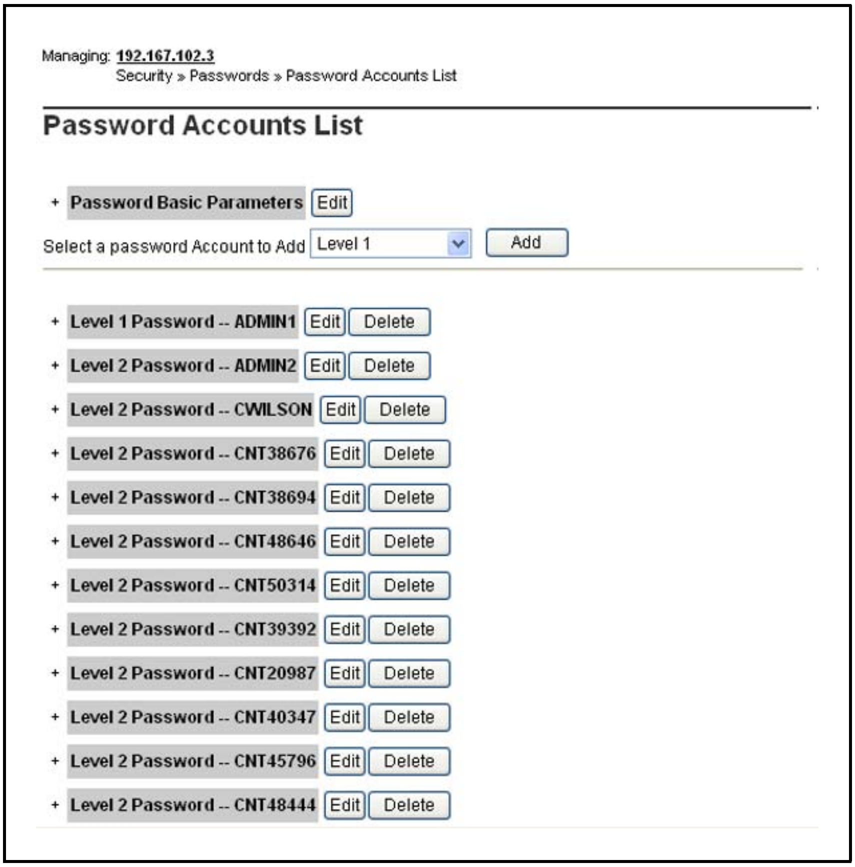
Use the procedures in this section to manage users, change passwords, and configure access restrictions using Element Manager. Users without the Administer Accounts privilege can change their own password only.

Add a user

Use the following two procedures to add user accounts.

Procedure 76
Adding a user other than LAPW by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List

Password Accounts List

+ Password Basic Parameters [Edit]

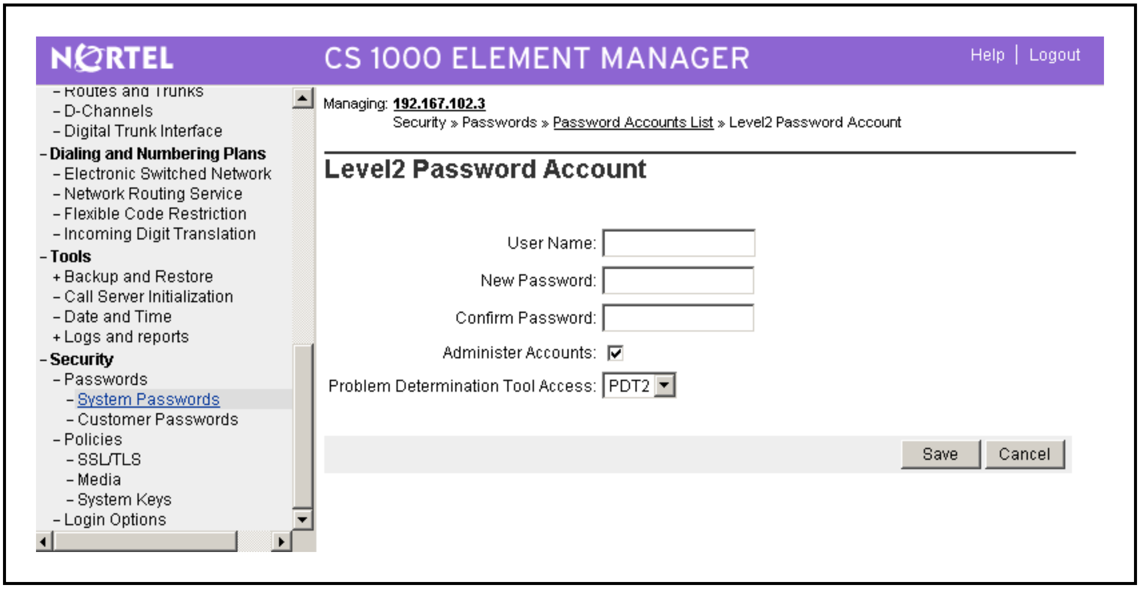
Select a password Account to Add: Level 1 [Add]

+ Level 1 Password -- ADMIN1 [Edit] [Delete]
+ Level 2 Password -- ADMIN2 [Edit] [Delete]
+ Level 2 Password -- CWILSON [Edit] [Delete]
+ Level 2 Password -- CNT38676 [Edit] [Delete]
+ Level 2 Password -- CNT38694 [Edit] [Delete]
+ Level 2 Password -- CNT48646 [Edit] [Delete]
+ Level 2 Password -- CNT50314 [Edit] [Delete]
+ Level 2 Password -- CNT39392 [Edit] [Delete]
+ Level 2 Password -- CNT20987 [Edit] [Delete]
+ Level 2 Password -- CNT40347 [Edit] [Delete]
+ Level 2 Password -- CNT45796 [Edit] [Delete]
+ Level 2 Password -- CNT48444 [Edit] [Delete]

3 From the **Select a password Account to Add** list, select one of the listed account types. For more information about the account types available, see “System accounts” (page 45).

4 Click **Add**.

The **Password Account** page appears. The page varies slightly depending on what type of account you selected.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List » Level2 Password Account

Level2 Password Account

User Name:
New Password:
Confirm Password:
Administer Accounts: ☑
Problem Determination Tool Access: PDT2

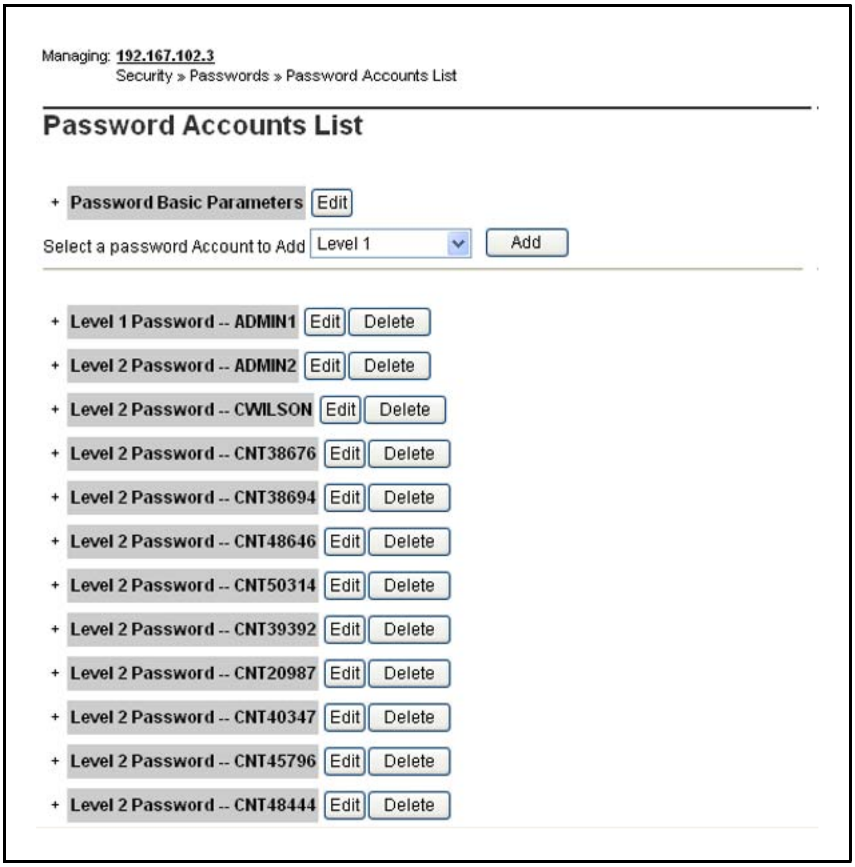
[Save] [Cancel]

5	Enter the user name in the **User name** field, and the password in the **New password** and **Confirm password** fields.
6	Choose from one or more of the following options, depending on the type of account you are adding: **a** If you are adding a Level 1 or Level 2 account, and want to give the user PDT access, make a selection in the **Problem Determination Tools Access** list. **b** If you are adding a Level 2 account, select or clear the **Administer Accounts** check box.
7	Click **Save** to save the new user, and return to the **Password Accounts List** page.

--End--

Procedure 77
Adding an LAPW user by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List

Password Accounts List

- + Password Basic Parameters

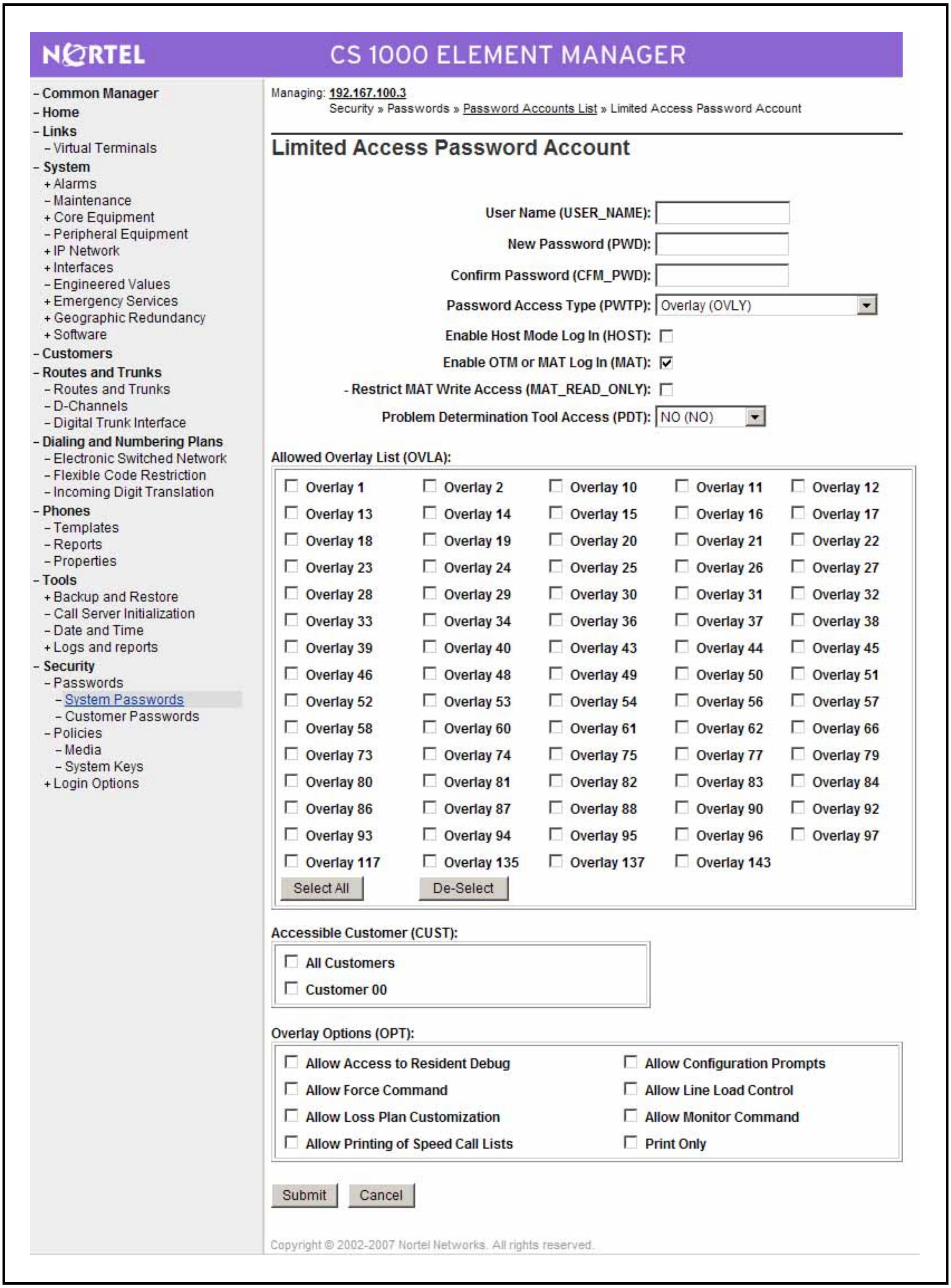
Select a password Account to Add: Level 1

- + Level 1 Password -- ADMIN1
- + Level 2 Password -- ADMIN2
- + Level 2 Password -- CWILSON
- + Level 2 Password -- CNT38676
- + Level 2 Password -- CNT38694
- + Level 2 Password -- CNT48646
- + Level 2 Password -- CNT50314
- + Level 2 Password -- CNT39392
- + Level 2 Password -- CNT20987
- + Level 2 Password -- CNT40347
- + Level 2 Password -- CNT45796
- + Level 2 Password -- CNT48444

3 From the **Select a password Account to Add** list, select **Limited Access**. For more information about the account types available, see “System accounts” (page 45).

4 Click **Add**.

The **Limited Access Password Account** page appears.



Managing: 192.167.100.3
Security » Passwords » Password Accounts List » Limited Access Password Account

Limited Access Password Account

User Name (USER_NAME):

New Password (PWD):

Confirm Password (CFM_PWD):

Password Access Type (PWTP): Overlay (OVLY)

Enable Host Mode Log In (HOST): □

Enable OTM or MAT Log In (MAT): ☑

- Restrict MAT Write Access (MAT_READ_ONLY): □

Problem Determination Tool Access (PDT): NO (NO)

Allowed Overlay List (OVLA):

□ Overlay 1 □ Overlay 2 □ Overlay 10 □ Overlay 11 □ Overlay 12
□ Overlay 13 □ Overlay 14 □ Overlay 15 □ Overlay 16 □ Overlay 17
□ Overlay 18 □ Overlay 19 □ Overlay 20 □ Overlay 21 □ Overlay 22
□ Overlay 23 □ Overlay 24 □ Overlay 25 □ Overlay 26 □ Overlay 27
□ Overlay 28 □ Overlay 29 □ Overlay 30 □ Overlay 31 □ Overlay 32
□ Overlay 33 □ Overlay 34 □ Overlay 36 □ Overlay 37 □ Overlay 38
□ Overlay 39 □ Overlay 40 □ Overlay 43 □ Overlay 44 □ Overlay 45
□ Overlay 46 □ Overlay 48 □ Overlay 49 □ Overlay 50 □ Overlay 51
□ Overlay 52 □ Overlay 53 □ Overlay 54 □ Overlay 56 □ Overlay 57
□ Overlay 58 □ Overlay 60 □ Overlay 61 □ Overlay 62 □ Overlay 66
□ Overlay 73 □ Overlay 74 □ Overlay 75 □ Overlay 77 □ Overlay 79
□ Overlay 80 □ Overlay 81 □ Overlay 82 □ Overlay 83 □ Overlay 84
□ Overlay 86 □ Overlay 87 □ Overlay 88 □ Overlay 90 □ Overlay 92
□ Overlay 93 □ Overlay 94 □ Overlay 95 □ Overlay 96 □ Overlay 97
□ Overlay 117 □ Overlay 135 □ Overlay 137 □ Overlay 143

Accessible Customer (CUST):

□ All Customers
□ Customer 00

Overlay Options (OPT):

□ Allow Access to Resident Debug □ Allow Configuration Prompts
□ Allow Force Command □ Allow Line Load Control
□ Allow Loss Plan Customization □ Allow Monitor Command
□ Allow Printing of Speed Call Lists □ Print Only

Copyright © 2002-2007 Nortel Networks. All rights reserved.

5 Type the new user name in the **User name** field.

6 Type the password for the new user in the **New password** and **Confirm password** fields.

7 In the **Password access type** list, choose either **Overlay (OVLY)** or **Set Based Administration (SBA)**.

8 Select or clear **Enable host mode log in**.

9 Select or clear **Enable OTM or MAT Log In (MAT_READ_ONLY):**

10 Select or clear **Restrict MAT Write Access (MAT_READ_ONLY):**

11 In the **Problem Determination Tool Access (PDT)** list, choose one of **NO**, **PDT1** or **PDT2**

12 Select or clear the various overlays in the **Allowed Overlay List (OVLA)** list. You can use the **Select All** and **De-Select** buttons to select or clear all of the overlays in a single step.

13 Select or clear the various customers in the **Accessible Customer (CUST)** list.

14 Select or clear the various options in the **Overlay Options (OPT)** list.

15 Click **Submit** to save the new user, and return to the **Password Accounts List** page.

--End--

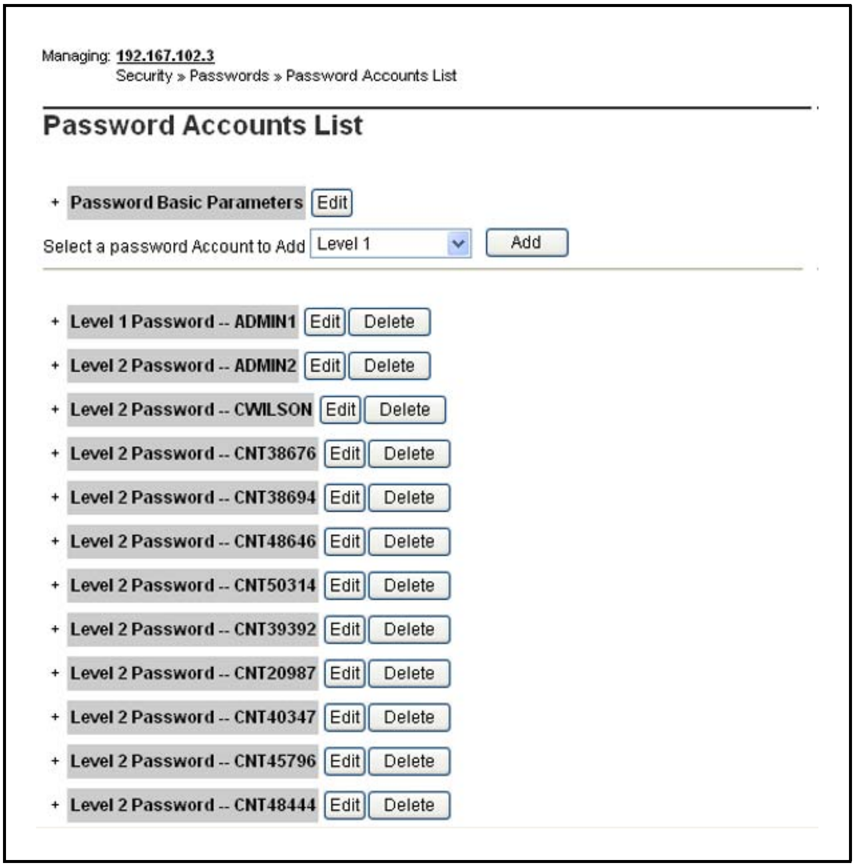
Edit an existing user

Use the following procedure to edit user accounts, including changing a user’s password.

To change passwords for Level 1 and Level 2 accounts, you must log on using an account that has Level 2 access.

Procedure 78
Editing an existing user by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List

Password Accounts List

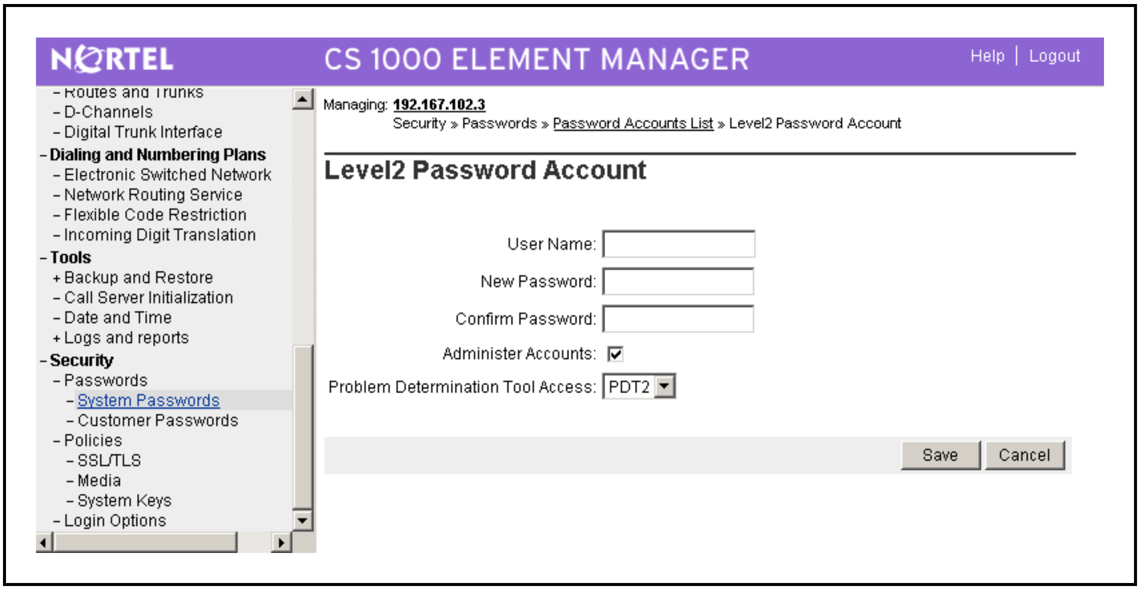
+ Password Basic Parameters [Edit]

Select a password Account to Add [Level 1] [Add]

+ Level 1 Password -- ADMIN1 [Edit] [Delete]
+ Level 2 Password -- ADMIN2 [Edit] [Delete]
+ Level 2 Password -- CWILSON [Edit] [Delete]
+ Level 2 Password -- CNT38676 [Edit] [Delete]
+ Level 2 Password -- CNT38694 [Edit] [Delete]
+ Level 2 Password -- CNT48646 [Edit] [Delete]
+ Level 2 Password -- CNT50314 [Edit] [Delete]
+ Level 2 Password -- CNT39392 [Edit] [Delete]
+ Level 2 Password -- CNT20987 [Edit] [Delete]
+ Level 2 Password -- CNT40347 [Edit] [Delete]
+ Level 2 Password -- CNT45796 [Edit] [Delete]
+ Level 2 Password -- CNT48444 [Edit] [Delete]

3 Next to the account you want to modify, click **Edit**.

The **Password Account** page appears.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List » Level2 Password Account

Level2 Password Account

User Name:
New Password:
Confirm Password:
Administer Accounts: ☑
Problem Determination Tool Access: PDT2

[Save] [Cancel]

Make changes to the password and access capabilities of the selected user by editing the fields and selecting or clearing the various options.

4 Click **Submit** to save your changes and return to the **Password Accounts List** page.

--End--

Synchronize a changed password

The Synchronize a changed password option is selected by default and prompts an EDD in the Call Server after the passwords are changed successfully. You must perform an EDD, or wait for the next scheduled EDD, to synchronize the password across the servers linked to the Call Server.

Manage passwords for stand-alone Signaling Server using NRS

Level 2 (PWD2) users manage accounts and passwords on the stand-alone Signaling Server running Network Routing Service (NRS).

Use the following procedure to access the PDT prompt on the stand-alone NRS. At the PDT prompt, you can execute OAM commands, as well as Nortel debug commands, and user and password management commands for the stand-alone NRS. For more information about user and password management commands available at the PDT prompt on the stand-alone NRS, see Table 52 "Job aid: user and password management commands on the stand-alone NRS" (page 241).

Procedure 79
Accessing the PDT prompt on stand-alone NRS

Step	Action
1	Log on to the NRS OAM shell using an account having admin privilege.
2	Access the PDT prompt by holding down the `ctrl` key, and typing `pdt`. The PDT prompt appears.

--End--

Table 52
Job aid: user and password management commands on the stand-alone NRS

Command	Description
adminUserPasswordChange [userID]	Use this command to give users the ability to change their own password, or to give a Level 2 (PWD2) user the ability to change any user password specified in the userID field. Requires Level 2 (PWD2) access.

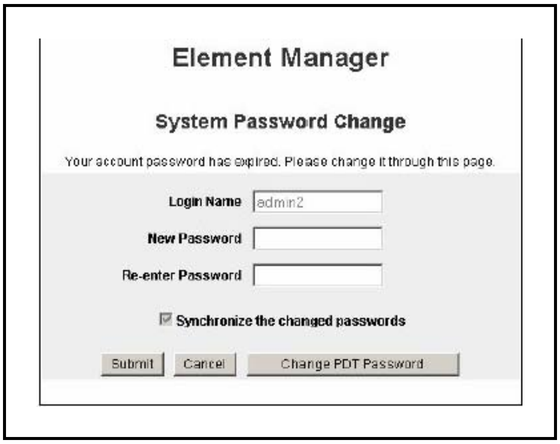
Table 52
Job aid: user and password management commands on the stand-alone NRS (cont'd.)

Command	Description
adminUserCreate [userID]	Use this command to create an account specified in the userID field. Requires Level 2 (PWD2) access.
adminUserDelete [userID]	Use this command to delete an account specified in the userID field. Requires Level 2 (PWD2) access.
adminAccountShow	Use this command to display all configured accounts on the system. Requires Level 2 (PWD2) access.

Change an expired password

If you log on using an expired password, you are directed immediately to the System Password Change facility of Element Manager. Enter a new password (and reenter it to conform the spelling), as shown in Figure 11 "System password change" (page 242).

Figure 11
System password change



Element Manager

System Password Change

Your account password has expired. Please change it through this page.

Login Name: admin2

New Password:

Re-enter Password:

☑ Synchronize the changed passwords

Edit global password settings

Use the following procedure to configure settings that apply to all accounts.

Table 53
Job aid: password options

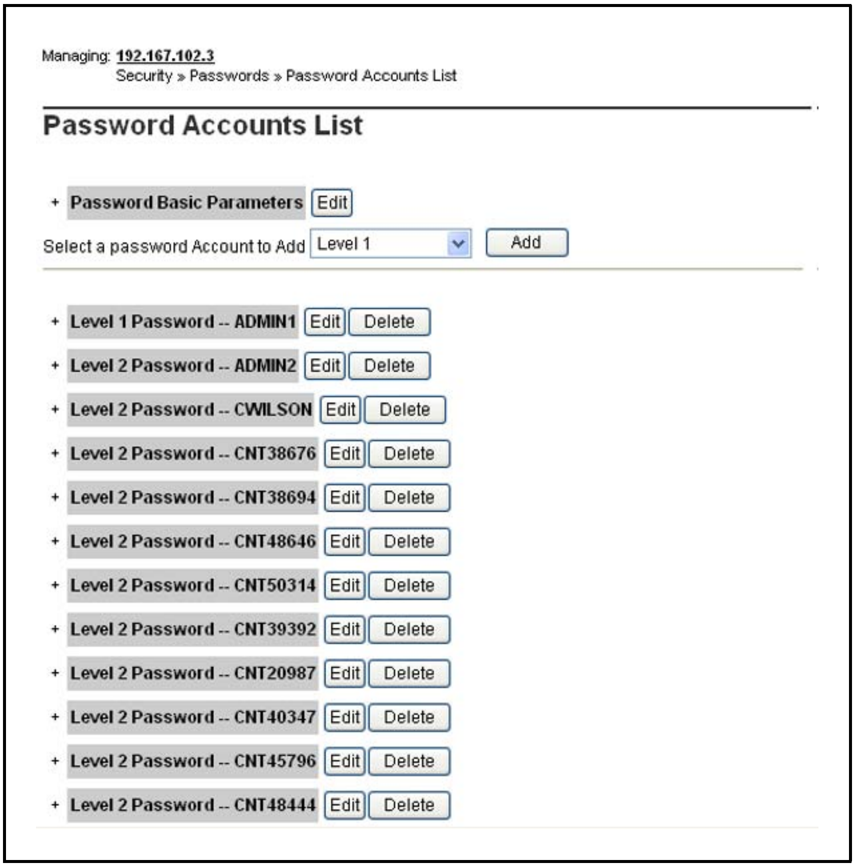
Password option	Effect
Force Password Change (FPC)	Prevents users from continuing to use the system default passwords.
Failed Log In Threshold	Controls the number of times a user can fail to log on before the port they are using is locked. To override a lockout, manually restart the system.

Password option	Effect
Failed Log In Threshold Alarm	Sets an alarm whenever the Failed Log in Threshold is exceeded.
Port Lockout Time After Failed Log in	Controls the length of time the port is locked after the Failed Log In Threshold value is reached.
Password Complexity Check	Tests user passwords to verify that they are difficult to guess.
Audit Trail for Password Usage	Prevents the reuse of a password.
Word Size of Audit Trail buffer	The size for the Audit Trail file, in the range of 50–1500. The default value is 50.
Last Log In Identification	Keeps track of the last user who logged on.
Inactivity Timeout	Ends a logon session after a period of inactivity.

For more information about the features described in this section, see "Global password settings" (page 48).

Procedure 80
Editing global password settings by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



Managing: 192.167.102.3
Security » Passwords » Password Accounts List

Password Accounts List

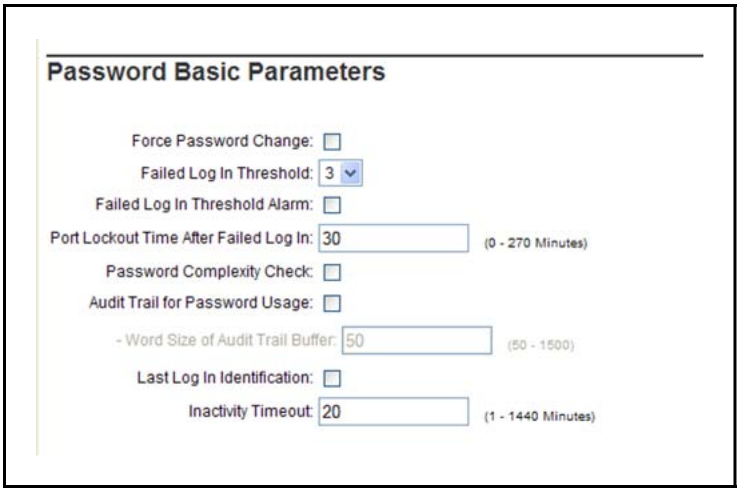
+ Password Basic Parameters [Edit]

Select a password Account to Add [Level 1 ▾] [Add]

+ Level 1 Password -- ADMIN1 [Edit] [Delete]
+ Level 2 Password -- ADMIN2 [Edit] [Delete]
+ Level 2 Password -- CWILSON [Edit] [Delete]
+ Level 2 Password -- CNT38676 [Edit] [Delete]
+ Level 2 Password -- CNT38694 [Edit] [Delete]
+ Level 2 Password -- CNT48646 [Edit] [Delete]
+ Level 2 Password -- CNT50314 [Edit] [Delete]
+ Level 2 Password -- CNT39392 [Edit] [Delete]
+ Level 2 Password -- CNT20987 [Edit] [Delete]
+ Level 2 Password -- CNT40347 [Edit] [Delete]
+ Level 2 Password -- CNT45796 [Edit] [Delete]
+ Level 2 Password -- CNT48444 [Edit] [Delete]

3 Next to **Password Basic Parameters**, click **Edit**.

The **Password Basic Parameters** page appears.



Password Basic Parameters

Force Password Change: □
Failed Log In Threshold: [3 ▾]
Failed Log In Threshold Alarm: □
Port Lockout Time After Failed Log In: 30 (0 - 270 Minutes)
Password Complexity Check: □
Audit Trail for Password Usage: □
- Word Size of Audit Trail Buffer: 50 (50 - 1500)
Last Log In Identification: □
Inactivity Timeout: 20 (1 - 1440 Minutes)

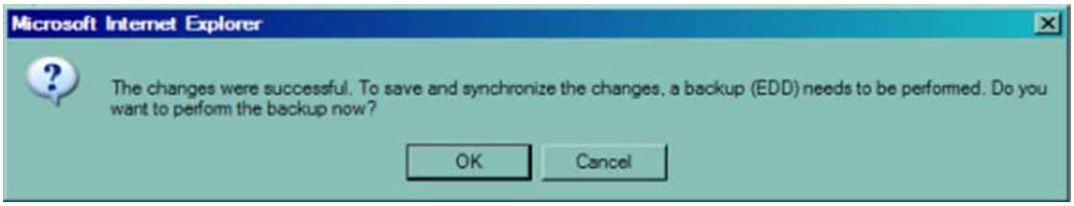
4 Edit any of the following parameters by selecting or clearing the check box, selecting from the list, or entering a value:

- Force Password Change
- Failed Log in Threshold
- Failed Log In Threshold Alarm

- Port Lockout Time After Failed Log in
- Password Complexity Check
- Audit Trail for Password Usage
- Word Size of Audit Trail buffer
- Last Log In Identification
- Inactivity Timeout

5 Click **Save** to save the changed password settings, and return to the **Password Accounts List** page.

The following message appears:



The changes were successful. To save and synchronize the changes, a backup (EDD) needs to be performed. Do you want to perform the backup now?

6 Click **OK** to perform an EDD.

--End--

When the Force Password Change (FPC) feature is On, PWD and PDT users logging on using default passwords must change their passwords before continuing. For more information about changing an expired password, see "Change an expired password " (page 242).

Security administration

This chapter contains procedures to help you manage system security and secure remote access features. The chapter is divided into the following sections:

- “Control access to the system” (page 247)
- “Add or remove elements from the UCM security domain” (page 249)
- “Authentication methods” (page 269)
- “Refresh system keys” (page 272)
- “Control access to system Application Processors” (page 273)
- “Configure Secure File Transfer Protocol” (page 274)
- “Configure port access restrictions” (page 277)
- “Configure remote access” (page 286)
- “Access the system remotely” (page 290)
- “SSH key synchronization between active and inactive cores” (page 291)
- “Manage SSH keys using overlays” (page 291)
- “SSH key management using Element Manager” (page 296)
- “Customize the logon banner” (page 297)
- “Force an EDD using overlays” (page 301)

Control access to the system

To limit unauthorized functional and physical access to the system and its network connections, arrange for:

- system administration port security (see “System administration port security” (page 248))
- switchroom security (see “Switchroom security” (page 248))
- network facilities security (see “Network facilities security” (page 249))

System administration port security

You can use remote system administration to access the system using maintenance modems or an on-site terminal. You can use this access method to adjust and troubleshoot system hardware and software components; however, this feature must be configured to discourage unauthorized users from using it to access the system remotely, alter the system configuration, steal services, and degrade system performance.

Unauthorized users can attempt to dial in to the remote access port, break the password, and reprogram system memory to permit international calls, enable Direct Inward System Access (DISA), turn off Call Detail Recording (CDR), traffic, and history reports, and either eliminate the need for Authcodes or create new Authcodes.

You can use port counters on the TTY and PRT ports to limit unauthorized access. If a user enters invalid characters, the port is disabled. The port is automatically reenabled after 4 minutes; this can occur a maximum of three times in 30 minutes. If a port is disabled four times in 30 minutes, you must reenable it manually.

Access to the system communication ports can be limited using passwords. For more information about configuring passwords to limit access to the ports, see “Password management” (page 224).

Switchroom security

Ensure that the room where the switch is physically located is secure, otherwise unauthorized users can access all system resources. Unauthorized users can take actions such as turning off printer and CDR processors or removing cards from the system, which renders the system inoperable. Follow these security procedures to minimize this risk:

- Limit access to the switchroom to authorized personnel only.
- Require distributor and telephone company personnel to sign in and out and provide identification, if necessary.
- Control, document, and audit major changes to system configuration.
- Require personnel to sign out parts and equipment.
- Store printouts of system configurations and databases in a secure, locked area.
- Do not post passwords or Trunk Access Codes in the switchroom.
- Keep the switchroom and telephone equipment closets locked.

Network facilities security

Network security is just as important as switchroom security. For example, unsecured facilities can be accessed using a test terminal to place unauthorized calls without these calls being detected by the system and recorded by the CDR.

Follow these security procedures to minimize this risk of misuse:

- Secure the telephone company access point, individual distribution frame location, and the Main Distribution Frame (MDF).
- Avoid locating Intermediate Distribution Frames (IDF) in janitorial, electrical, and supply closets. Limit access when collocation is unavoidable.
- Document existing outside and inside cable plans and update these records as service changes are made.
- Where cable plan records do not exist, consider hiring an independent consultant to verify and document the cable plan.
- Maintain and document all moves and changes. Eliminate all out-of-service cross connects if not using the Automatic Set Relocation feature.
- Encase and lock building entry terminals and secure manholes.
- Avoid posting cable documentation in the IDF.
- Keep cable plant documentation in at least two separate secure locations.
- Verify terminal connections against cable plant and system records, and resolve all differences.
- Audit the entire system, ensuring that all cable, telephone company, telephone, and system records are accurate.
- Limit access to the ELAN using firewalls or appropriate data network configuration. Physical access and data network access to the ELAN is recommended to protect the system from attacks.

Add or remove elements from the UCM security domain

Use the commands inTable 54 "Commands for adding or removing elements from the UCM security domain" (page 250) to add or remove elements from the Unified Communications Management security domain.

Before issuing the commands to join the security domain, ensure that all elements are active and known to the Call Server.

Table 54
Commands for adding or removing elements from the UCM security domain

Command	Type	Preconditions	Description
`joinSecDomain`	OAM/PDT CLI	• PWD2 privilege • UCM security IP address • Username and password for a UCM administrator whose UCM role includes the Security Administrator	Establish mutual trust with the primary security server.
`leaveSecDomain`	OAM/PDT CLI	• PWD2 privilege • Member of UCM security domain	Remove the primary security server mutual trust information from the device.
`statSecDomain`	OAM/PDT CLI	• PWD2 privilege • Member of UCM security domain	Display the primary security server IP address and fingerprint.
`Register UCMSecurity Device`	LD 117	• PWD2 privilege • UCM security IP address • Username and password for a UCM administrator whose UCM role includes the Security Administrator Linux base element	Establish mutual trust with the primary security server for the element. (If the system is a redundant system, the inactive Call Server joins the security domain automatically.)
`Register UCMSecurity System`	LD 117	• PWD2 privilege • UCM security IP address • username and password for a UCM administrator whose UCM role includes the Security Administrator Linux base element	All associated elements, such as MGCs and VGMCs, join the UCM security domain after prompting for user approval. (If the system is a redundant system, the inactive Call Server joins the security domain automatically.)
`Leave UCMSecurity Device`	LD 117	• Member of UCM security domain	Remove the primary security server mutual trust information from the system for the element. (If the system is a redundant system, the inactive CS leaves the security domain automatically.)

Command	Type	Preconditions	Description
			All associated elements, such as MGCs and VGMCs, leave the UCM security domain after prompting for user approval.
`Leave UCMSecurity System`	LD 117	• Member of UCM security domain	Remove the primary security server mutual trust information for the entire CS 1000 system.
`Stat UCMSecurity`	LD 117	• No privilege requirement • Member of UCM security domain	Display the primary security server IP address and fingerprint.
`Stat UCMSecurity System [Refresh]`	LD 117	• No privilege requirement • Member of UCM security domain	Display all known CS 1000 elements (such as MGC, MC32, MC32S) and their current UCM security domain status as Registered or Unregistered. Use [Refresh] to refresh the list.

Note 1: When you reboot Media Gateway devices after upgrade (except for MC32S), log messages dsLOG003 tAccountTransfer and LOG003 tBannerTransfer display due to the account database and banner file transfer failing while the device waits to register with the UCM security domain.

Note 2: PWD2 is the pre-membership system password. It no longer exists once the system joins the security domain.

VxWorks systems and devices

VxWorks based systems and devices can join the Unified Communications Management security domain using the following modes:

- Manual mode—the joining and leaving of the Unified Communications Management security domain operation is performed on each individual Call Server, MGC and VGMC using the following commands:
  - — LD 117 command: **`[REGISTER / UNREGISTER] UCMSECURITY DEVICE`**
  - — OAM/PDT/IPL commands: **`joinSecDomain`** or **`leaveSecDomain`**
- User mode—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:

— LD 117 command: `[REGISTER / UNREGISTER] UCMSECURITY SYSTEM`

Adding elements to the security domain when ISSS is enabled

Before adding a non-Linux element (such as Media Card and MGC) to a security domain where ISSS is enabled, do the following:

- Add a new manual IPsec target with the IP address as the ELAN IP address of the non-Linux element. Ensure that the **Enable IPSec** check box is not selected.
- Synchronize and activate the IPsec configuration using Graceful mode.

For procedures related to ISSS, see "IPsec configuration" (page 74).

> ***Note:*** If adding a pre-Release 6.0 Gold MGC to a Release 6.0 system that has ISSS enabled in FULL mode and is hardened, you must enable FTP as it is disabled on the Call Server and Signaling Server during the hardening process (sFTP is used by default). FTP is required for updating the loadware on the card, which enables it to register to the UCM security domain.

This process allows the non-Linux element to communicate with the Call Server or Element Manager without using IPsec so that any required updates can be applied to the element prior to registering with the security domain. The manual IPsec target is replaced with the correct automatic target when the element registers with UCM.

If you are replacing a non-Linux element (such as Media Card and MGC), instead of adding a new manual ISSS target you must disable IPsec for the appropriate automatic target in UCM. Do this as follows:

- Select the radio button beside the target being replaced and click **IPSec Not Required**.
- Synchronize and activate the IPsec configuration using Graceful mode.

To minimize the required steps during an upgrade or new installation, Nortel recommends that you register all (or most) elements before enabling ISSS.

Co-resident Call Server and Signaling Server systems

Co-resident systems can join the Unified Communications Management security domain using the following modes:

- User mode—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:

— LD 117 command: `[REGISTER / UNREGISTER] UCMSECURITY SYSTEM`

This command can only be used to join the associated MGCs and VGMCs to the security domain and not the Call Server itself. In the Co-resident Call Server and Signaling Server configuration, the Call Server is joined to the security domain with Linux base during installation.

Join a Co-resident Signaling Server to the UCM security domain using Base Manager

You can use Base Manager to join a Co-resident Signaling Server to the UCM security domain.

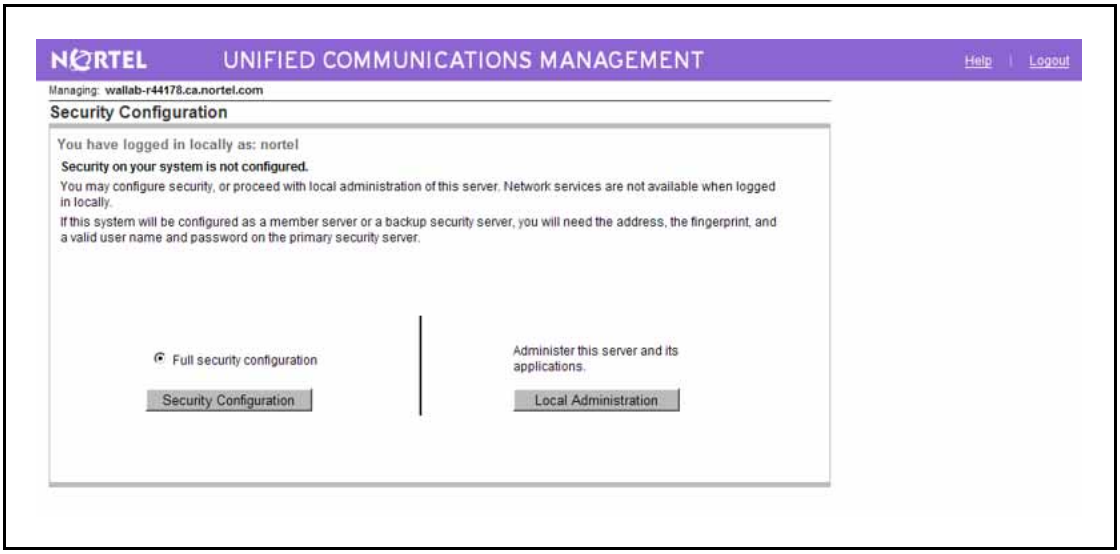
You must join the Signaling Servers to the UCM security domain in the following order:

- Primary server
- Backup server
- Member server

For the procedure to login and access the Base Manager application, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Procedure 81
Joining a Primary security server to the UCM security domain using Base Manager

Step	Action
1	From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**.



Managing: wallab-r44178.ca.nortel.com

Security Configuration

You have logged in locally as: nortel

Security on your system is not configured.

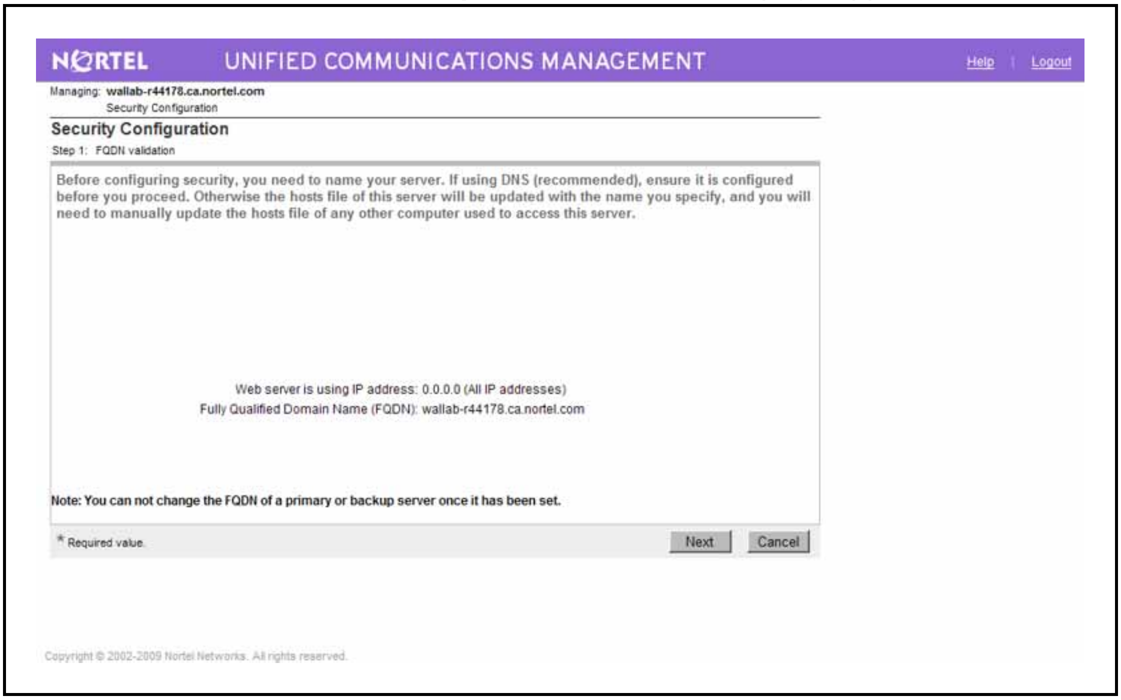
You may configure security, or proceed with local administration of this server. Network services are not available when logged in locally.

If this system will be configured as a member server or a backup security server, you will need the address, the fingerprint, and a valid user name and password on the primary security server.

● Full security configuration

Administer this server and its applications.

The **Step 1: FQDN validation** page appears.



NORTEL UNIFIED COMMUNICATIONS MANAGEMENT Help | Logout

Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration

Step 1: FQDN validation

Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.

Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): wallab-r44178.ca.nortel.com

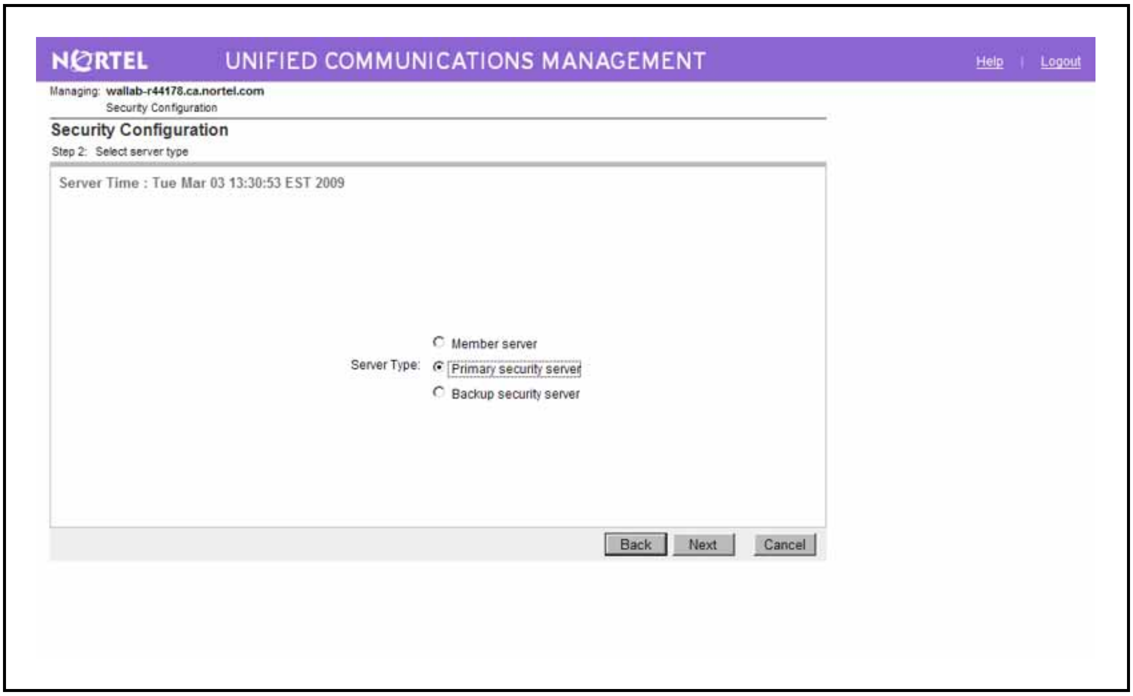
Note: You can not change the FQDN of a primary or backup server once it has been set.

* Required value. Next Cancel

Copyright © 2002-2009 Nortel Networks. All rights reserved.

2 Click **Next**.

The **Step 2: Select server type** page appears.



NORTEL UNIFIED COMMUNICATIONS MANAGEMENT Help | Logout

Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration

Step 2: Select server type

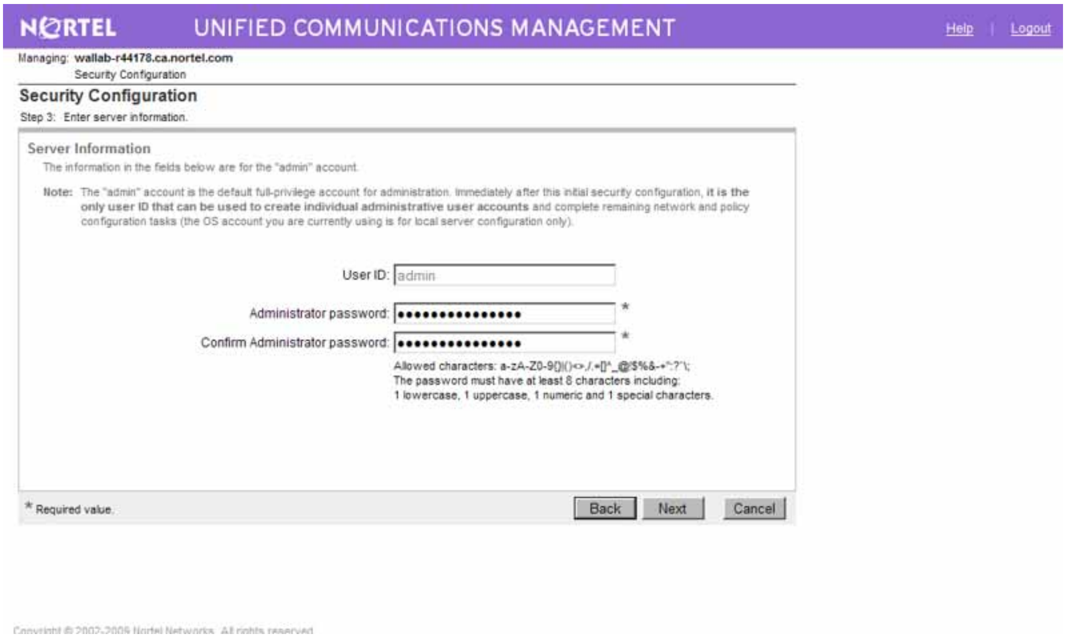
Server Time : Tue Mar 03 13:30:53 EST 2009

Server Type:
○ Member server
● Primary security server
○ Backup security server

Back Next Cancel

3 Select the **Primary security server** radio button and click **Next**.

The **Step 3: Enter server information** page appears.



Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration

Step 3: Enter server information.

Server Information

The information in the fields below are for the "admin" account.

Note: The "admin" account is the default full-privilege account for administration. Immediately after this initial security configuration, **it is the only user ID that can be used to create individual administrative user accounts** and complete remaining network and policy configuration tasks (the OS account you are currently using is for local server configuration only).

User ID: admin

Administrator password: ●●●●●●●●●●●●●●● *

Confirm Administrator password: ●●●●●●●●●●●●●●● *

Allowed characters: a-zA-Z0-9{}|()<>,/.=[]^_@/$%&-+":?`\;
The password must have at least 8 characters including:
1 lowercase, 1 uppercase, 1 numeric and 1 special characters.

* Required value.

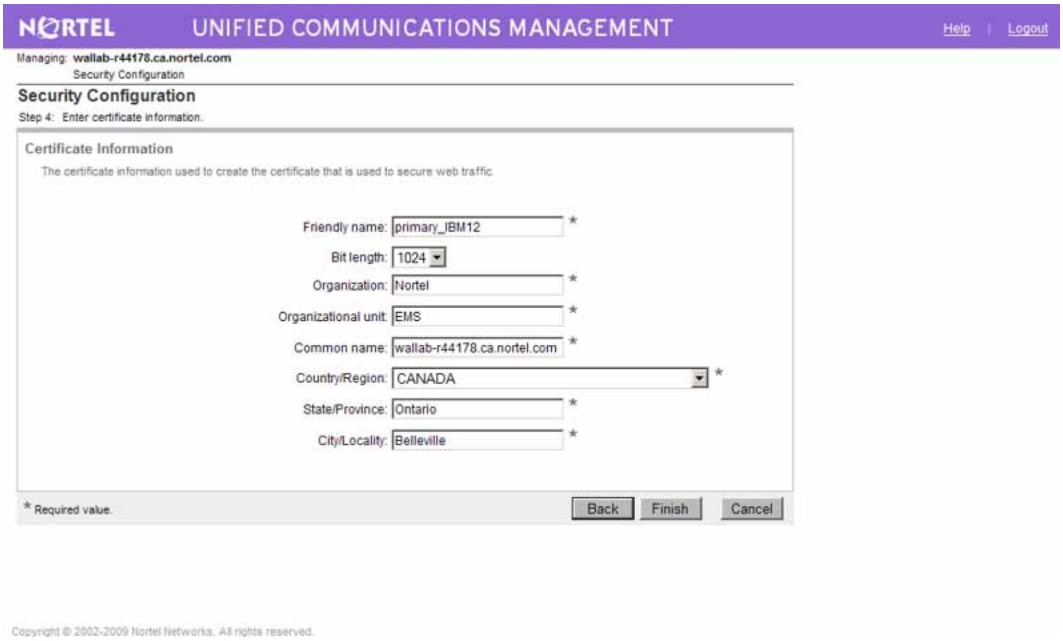
Copyright © 2002-2009 Nortel Networks. All rights reserved.

4 Enter the following information into the appropriate fields:

- UserID
- Administrator password
- Confirm Administrator password

5 Click **Next**.

The **Step 4: Enter certificate information** page appears.



Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration

Step 4: Enter certificate information.

Certificate Information

The certificate information used to create the certificate that is used to secure web traffic.

Friendly name: primary_IBM12 *

Bit length: 1024

Organization: Nortel *

Organizational unit: EMS *

Common name: wallab-r44178.ca.nortel.com *

Country/Region: CANADA *

State/Province: Ontario *

City/Locality: Belleville *

* Required value.

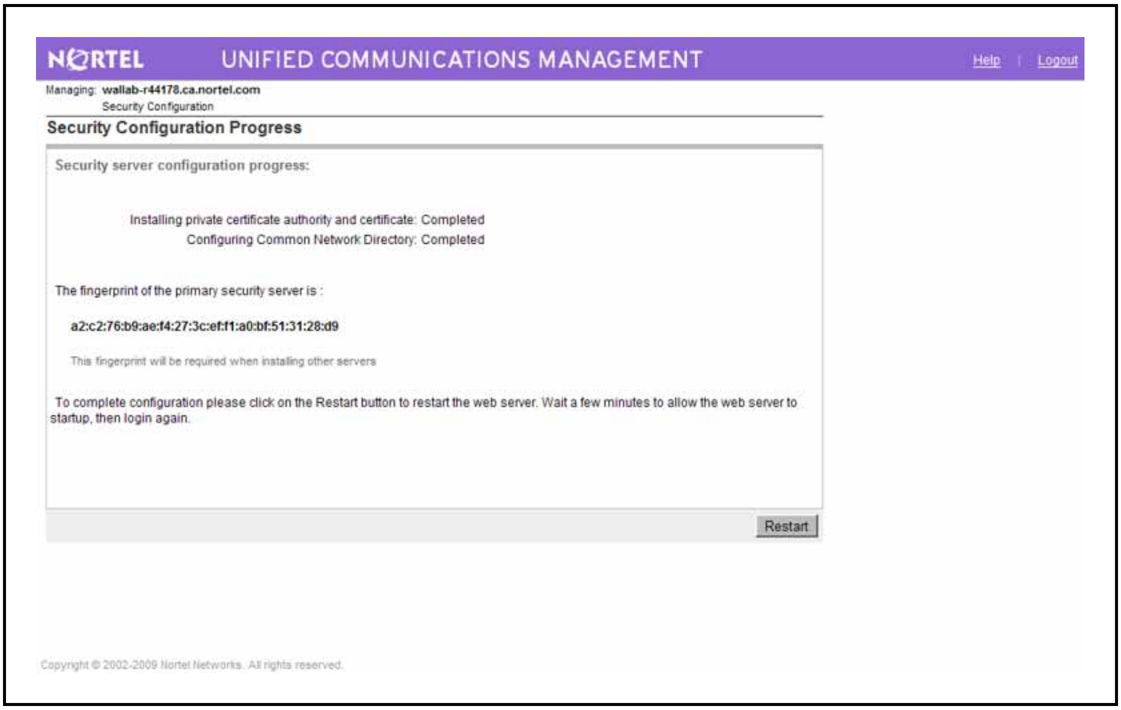
Copyright © 2002-2009 Nortel Networks. All rights reserved.

6 Enter the following information into the appropriate fields:

- Friendly name
- Bit length
- Organization
- Organizational unit
- Common name
- Country/Region
- State/Province
- City/Locality

7 Click **Finish**.

The **Security Configuration Progress** page appears.



Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration Progress

Security server configuration progress:

Installing private certificate authority and certificate: Completed
Configuring Common Network Directory: Completed

The fingerprint of the primary security server is :

a2:c2:76:b9:ae:f4:27:3c:ef:f1:a0:bf:51:31:28:d9

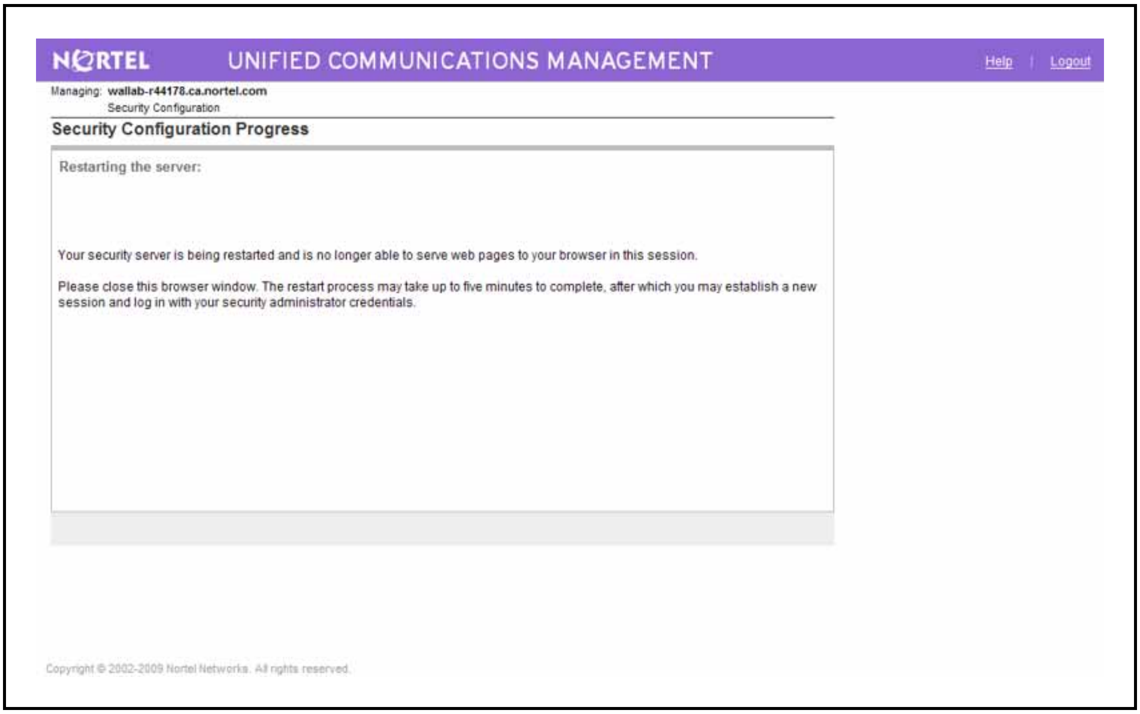
This fingerprint will be required when installing other servers

To complete configuration please click on the Restart button to restart the web server. Wait a few minutes to allow the web server to startup, then login again.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

8 To complete the configuration process, you must restart the web server. Click **Restart**.

The **Security Configuration Progress** page confirms that the server is restarting.



Managing: wallab-r44178.ca.nortel.com
Security Configuration

Security Configuration Progress

Restarting the server:

Your security server is being restarted and is no longer able to serve web pages to your browser in this session.

Please close this browser window. The restart process may take up to five minutes to complete, after which you may establish a new session and log in with your security administrator credentials.

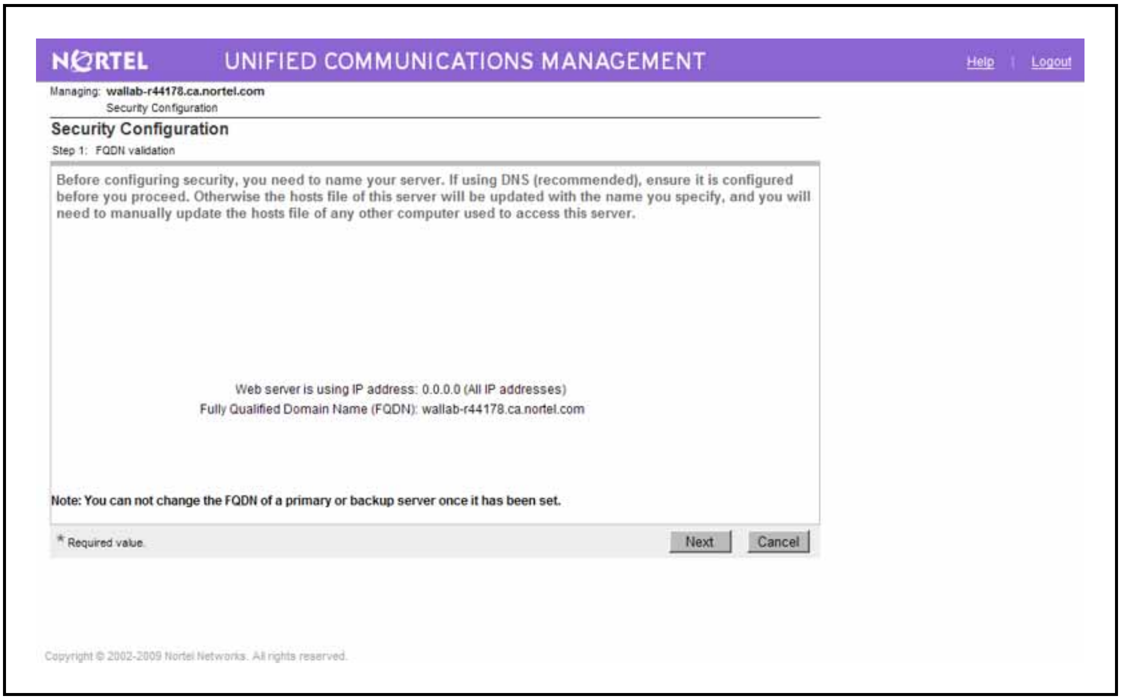
Copyright © 2002-2009 Nortel Networks. All rights reserved.

The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

--End--

Procedure 82
Joining a Backup security server to the UCM security domain using Base Manager

Step	Action
1	From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**. The **Step 1: FQDN validation** page appears.



Managing: wallab-r44178.ca.nortel.com
Security Configuration

Security Configuration

Step 1: FQDN validation

Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.

Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): wallab-r44178.ca.nortel.com

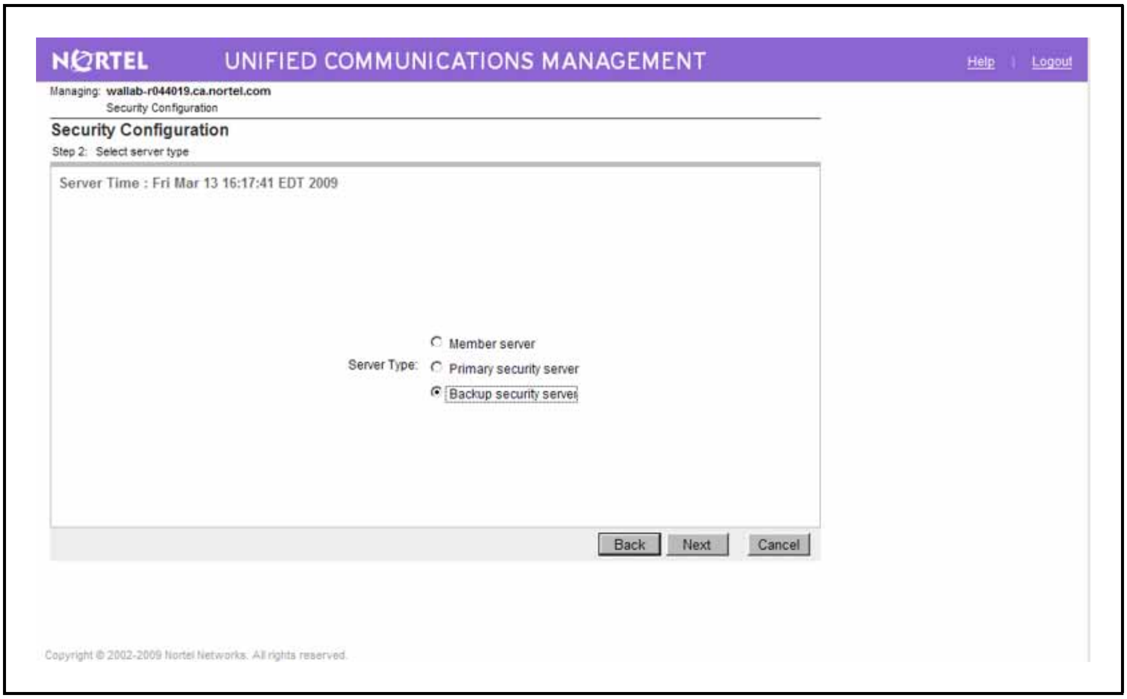
Note: You can not change the FQDN of a primary or backup server once it has been set.

* Required value.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

2 Click **Next**.

The **Step 2: Select server type** page appears.



Managing: wallab-r044019.ca.nortel.com
Security Configuration

Security Configuration

Step 2: Select server type

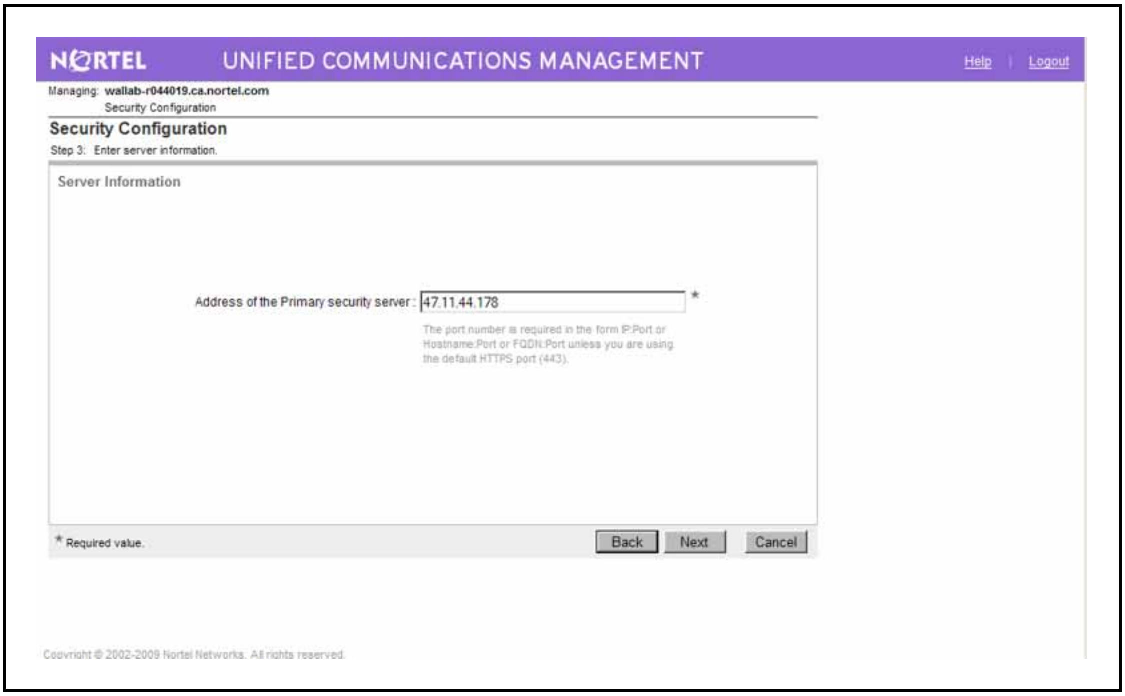
Server Time : Fri Mar 13 16:17:41 EDT 2009

Server Type: ○ Member server
○ Primary security server
● Backup security server

Copyright © 2002-2009 Nortel Networks. All rights reserved.

3 Select the **Backup security server** radio button and click **Next**.

The **Step 3: Enter server information** page appears.



Managing: **wallab-r044019.ca.nortel.com**
Security Configuration

Security Configuration

Step 3: Enter server information.

Server Information

Address of the Primary security server: 47.11.44.178 *

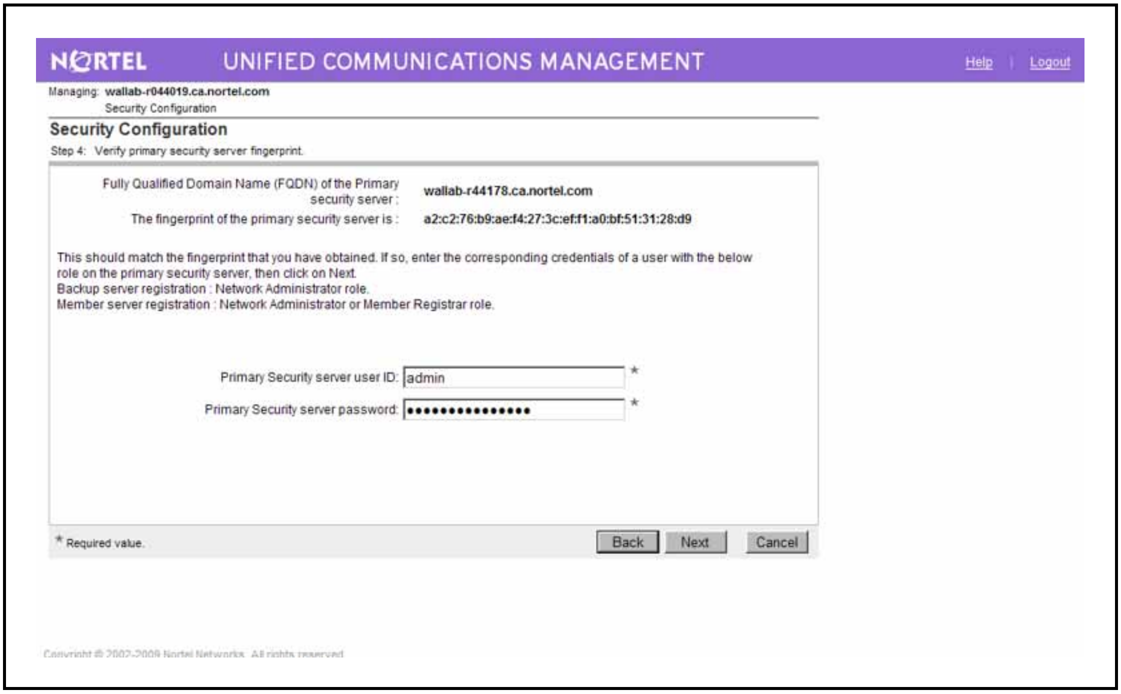
The port number is required in the form IP:Port or Hostname:Port or FQDN:Port unless you are using the default HTTPS port (443).

* Required value.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

4 Enter the IP address of the Primary security server and click **Next**.

The **Step 4: Verify primary security server fingerprint** page appears.



Managing: **wallab-r044019.ca.nortel.com**
Security Configuration

Security Configuration

Step 4: Verify primary security server fingerprint.

Fully Qualified Domain Name (FQDN) of the Primary security server: **wallab-r44178.ca.nortel.com**

The fingerprint of the primary security server is: **a2:c2:76:b9:ae:f4:27:3c:ef:f1:a0:bf:51:31:28:d9**

This should match the fingerprint that you have obtained. If so, enter the corresponding credentials of a user with the below role on the primary security server, then click on Next.
Backup server registration : Network Administrator role.
Member server registration : Network Administrator or Member Registrar role.

Primary Security server user ID: admin *

Primary Security server password: ●●●●●●●●●●●●●●● *

* Required value.

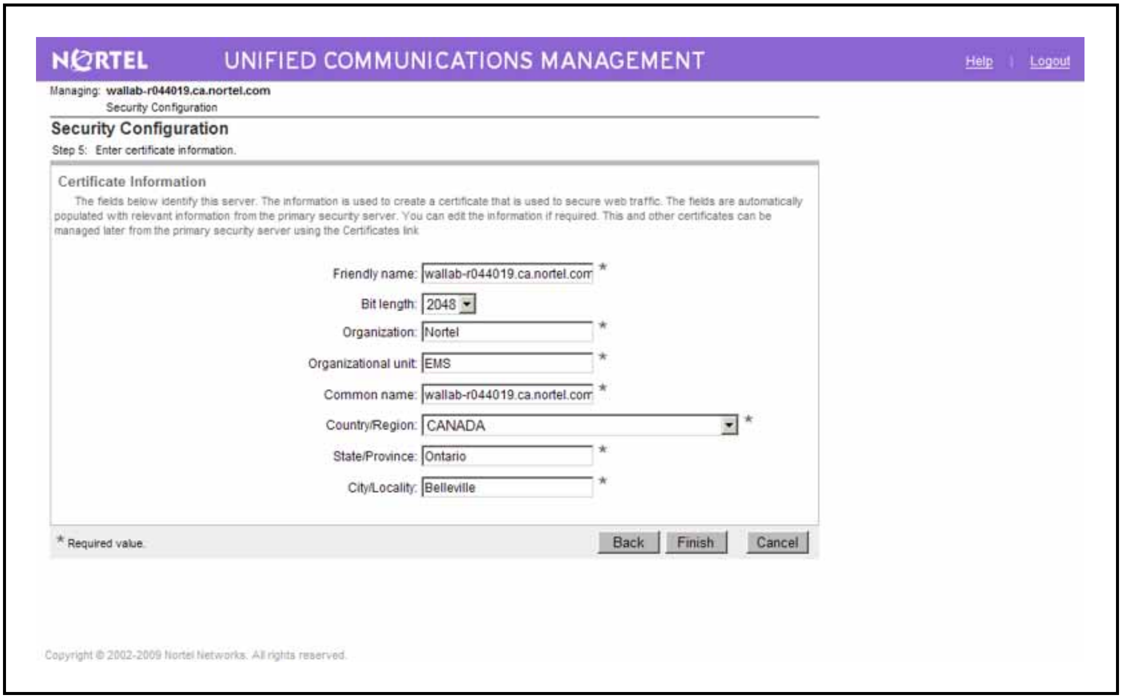
Copyright © 2002-2009 Nortel Networks. All rights reserved.

5 Verify that the FQDN and fingerprint information for the primary security server is valid and enter the following into the appropriate fields:

- Primary Security server user ID
- Primary Security server password

6 Click **Next**.

The **Step 5: Enter certificate information** page appears.



Managing: **wallab-r044019.ca.nortel.com**
Security Configuration

Security Configuration

Step 5: Enter certificate information.

Certificate Information

The fields below identify this server. The information is used to create a certificate that is used to secure web traffic. The fields are automatically populated with relevant information from the primary security server. You can edit the information if required. This and other certificates can be managed later from the primary security server using the Certificates link

Friendly name: wallab-r044019.ca.nortel.com *
Bit length: 2048
Organization: Nortel *
Organizational unit: EMS *
Common name: wallab-r044019.ca.nortel.com *
Country/Region: CANADA *
State/Province: Ontario *
City/Locality: Belleville *

* Required value.

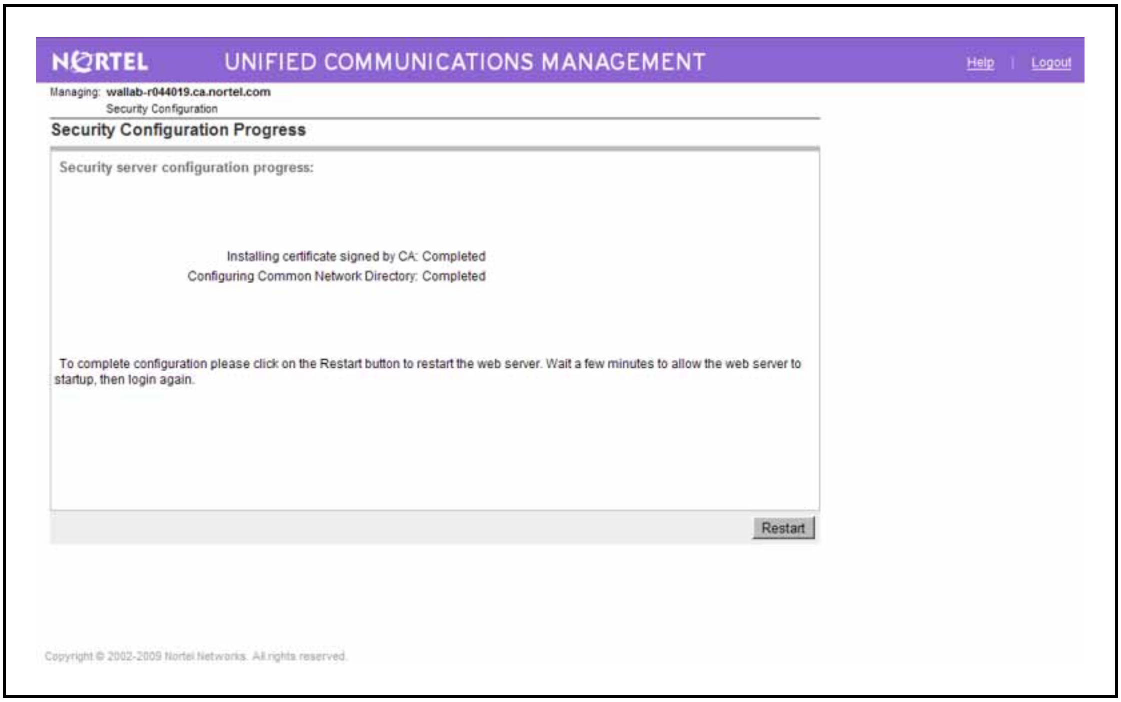
Copyright © 2002-2009 Nortel Networks. All rights reserved.

7 Enter the following information into the appropriate fields:

- Friendly name
- Bit length
- Organization
- Organizational unit
- Common name
- Country/Region
- State/Province
- City/Locality

8 Click **Finish**.

The **Security Configuration Progress** page appears.



Managing: wallab-r044019.ca.nortel.com
Security Configuration

Security Configuration Progress

Security server configuration progress:

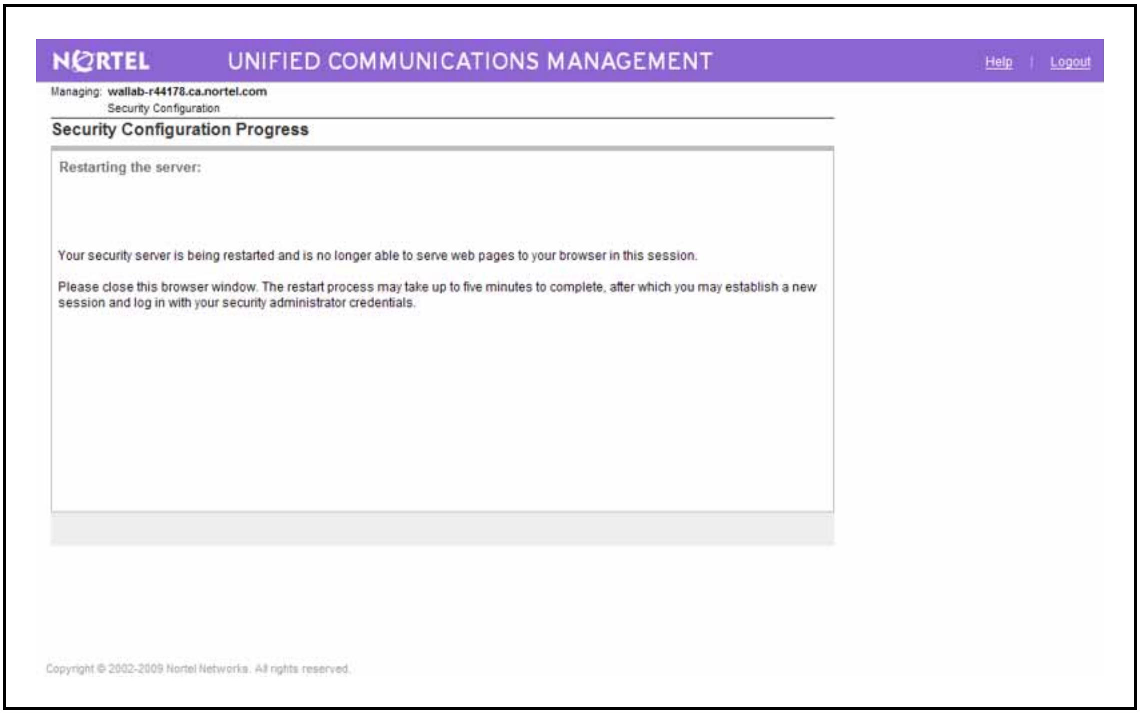
Installing certificate signed by CA: Completed
Configuring Common Network Directory: Completed

To complete configuration please click on the Restart button to restart the web server. Wait a few minutes to allow the web server to startup, then login again.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

9 To complete the configuration process, you must restart the web server. Click **Restart**.

The **Security Configuration Progress** page confirms that the server is restarting.



Managing: wallab-r44178.ca.nortel.com
Security Configuration

Security Configuration Progress

Restarting the server:

Your security server is being restarted and is no longer able to serve web pages to your browser in this session.

Please close this browser window. The restart process may take up to five minutes to complete, after which you may establish a new session and log in with your security administrator credentials.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

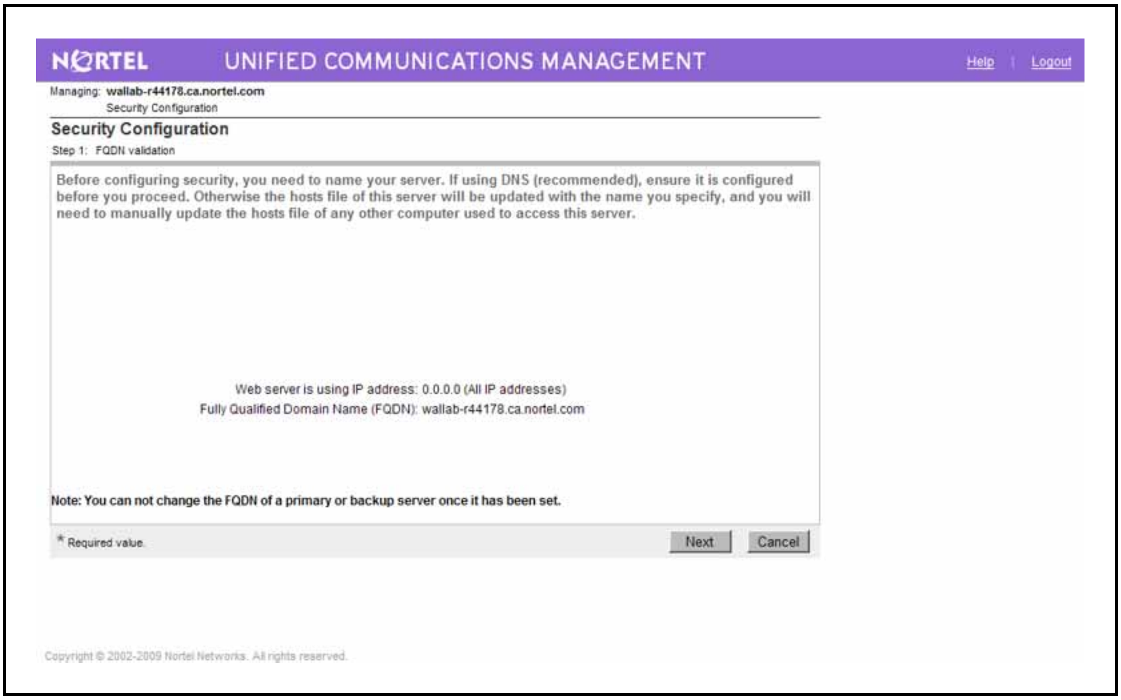
The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

--End--

Procedure 83
Joining a member server to the UCM security domain using Base Manager

Step	Action
1	From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**.

The **Step 1: FQDN validation** page appears.



Managing: **wallab-r44178.ca.nortel.com**
Security Configuration

Security Configuration

Step 1: FQDN validation

Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.

Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): wallab-r44178.ca.nortel.com

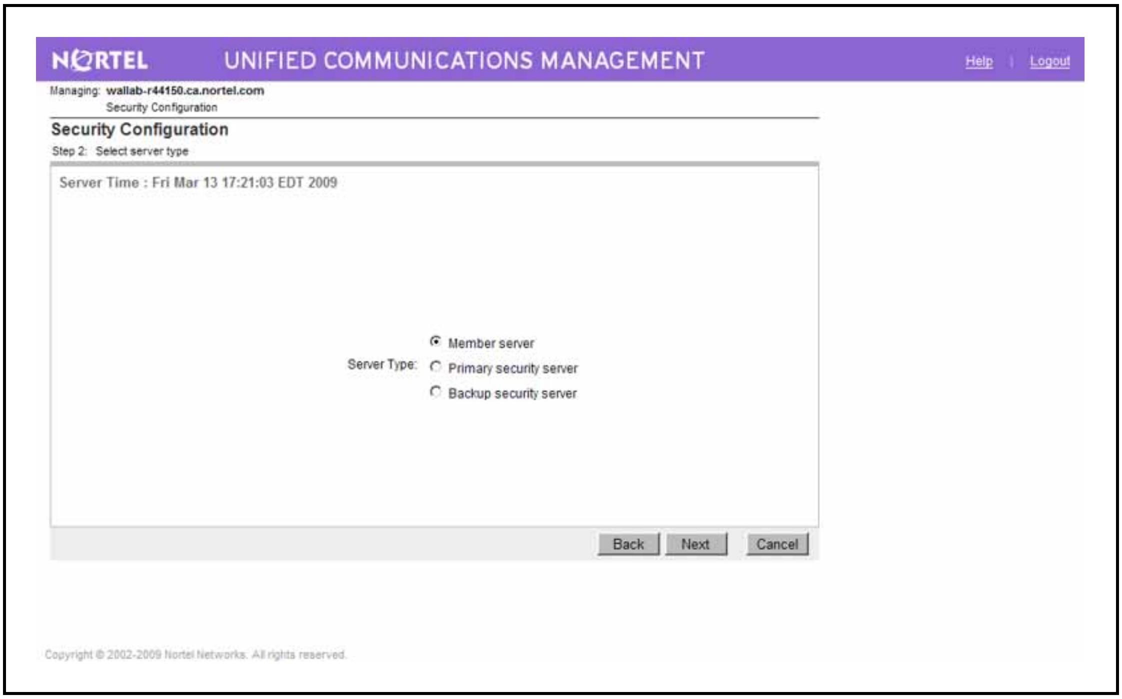
Note: You can not change the FQDN of a primary or backup server once it has been set.

* Required value.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

2 Click **Next**.

The **Step 2: Select server type** page appears.



Managing: wallab-r44150.ca.nortel.com
Security Configuration

Security Configuration

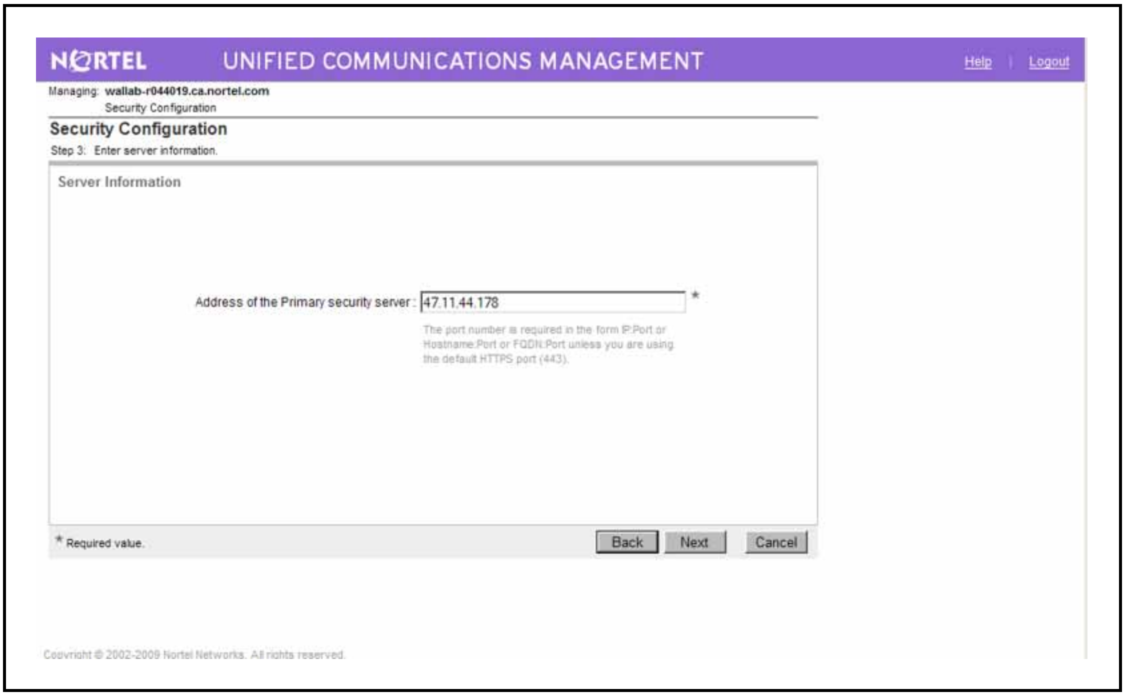
Step 2: Select server type

Server Time : Fri Mar 13 17:21:03 EDT 2009

Server Type: ● Member server
○ Primary security server
○ Backup security server

3 Select the **Member server** radio button and click **Next**.

The **Step 3: Enter server information** page appears.



Managing: wallab-r044019.ca.nortel.com
Security Configuration

Security Configuration

Step 3: Enter server information.

Server Information

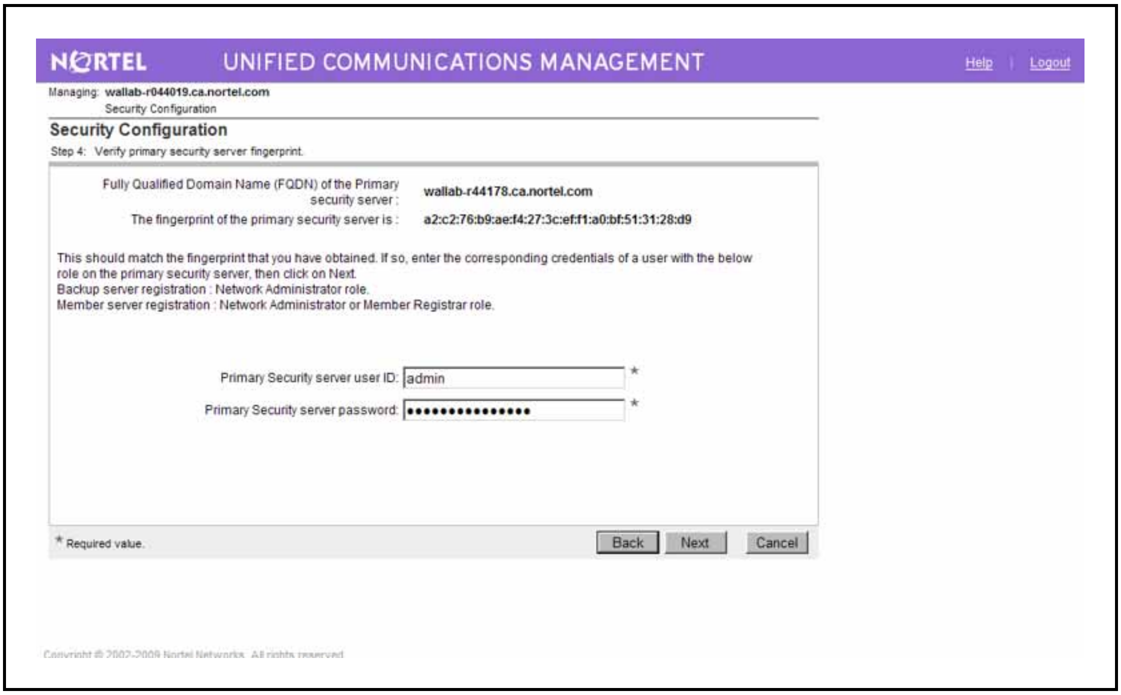
Address of the Primary security server: 47.11.44.178 *

The port number is required in the form IP:Port or Hostname:Port or FQDN:Port unless you are using the default HTTPS port (443).

* Required value.

4 Enter the IP address of the Primary security server and click **Next**.

The **Step 4: Verify primary security server fingerprint** page appears.



Managing: **wallab-r044019.ca.nortel.com**
Security Configuration

Security Configuration

Step 4: Verify primary security server fingerprint.

Fully Qualified Domain Name (FQDN) of the Primary security server : **wallab-r44178.ca.nortel.com**

The fingerprint of the primary security server is : **a2:c2:76:b9:ae:f4:27:3c:ef:f1:a0:bf:51:31:28:d9**

This should match the fingerprint that you have obtained. If so, enter the corresponding credentials of a user with the below role on the primary security server, then click on Next.
Backup server registration : Network Administrator role.
Member server registration : Network Administrator or Member Registrar role.

Primary Security server user ID: admin *

Primary Security server password: ••••••••••••••• *

* Required value.

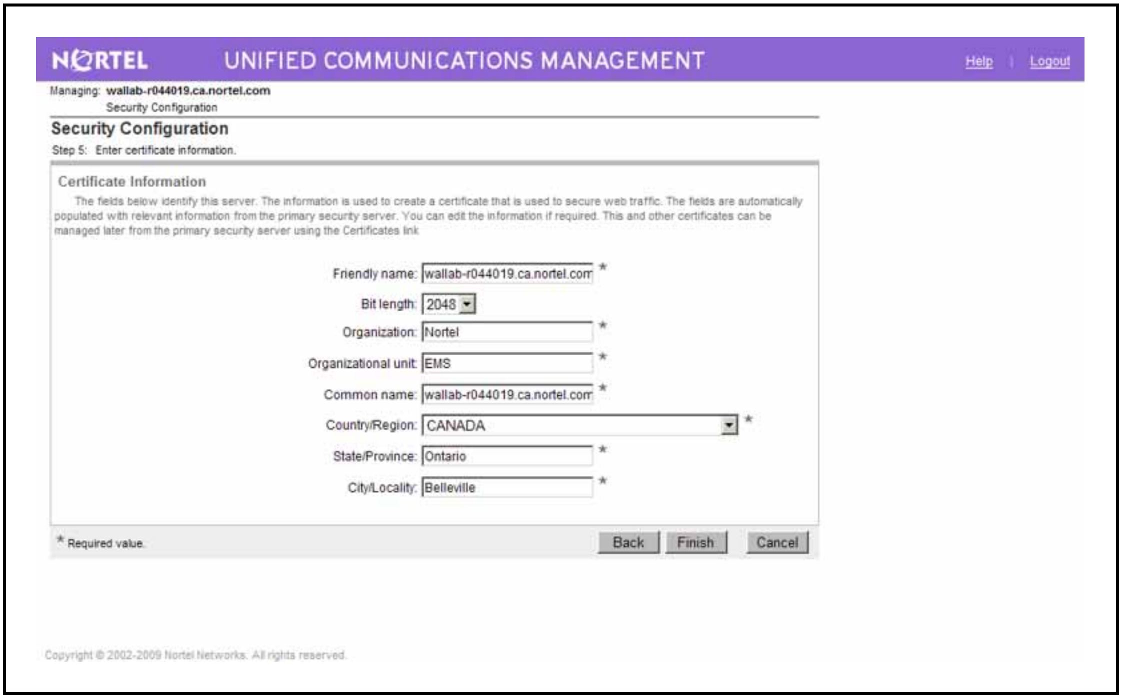
Copyright © 2002-2009 Nortel Networks. All rights reserved.

5 Verify that the FQDN and fingerprint information for the primary security server is valid and enter the following into the appropriate fields:

- Primary Security server user ID
- Primary Security server password

6 Click **Next**.

The **Step 5: Enter certificate information** page appears.



Managing: **wallab-r044019.ca.nortel.com**
Security Configuration

Security Configuration

Step 5: Enter certificate information.

Certificate Information

The fields below identify this server. The information is used to create a certificate that is used to secure web traffic. The fields are automatically populated with relevant information from the primary security server. You can edit the information if required. This and other certificates can be managed later from the primary security server using the Certificates link

Friendly name: wallab-r044019.ca.nortel.com *

Bit length: 2048

Organization: Nortel *

Organizational unit: EMS *

Common name: wallab-r044019.ca.nortel.com *

Country/Region: CANADA *

State/Province: Ontario *

City/Locality: Belleville *

* Required value.

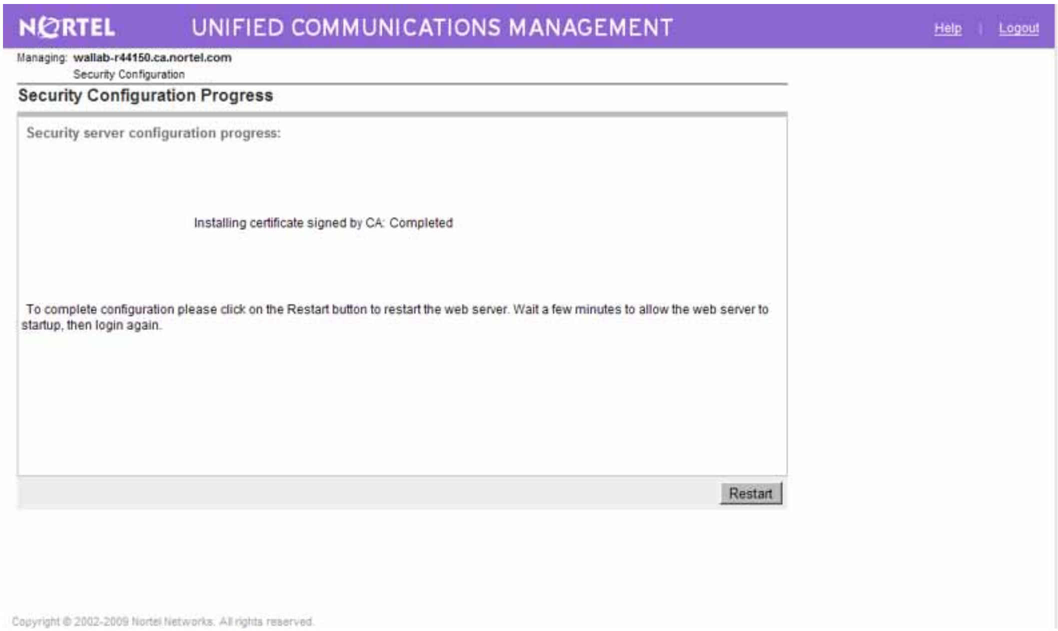
Copyright © 2002-2009 Nortel Networks. All rights reserved.

7 Enter the following information into the appropriate fields:

- Friendly name
- Bit length
- Organization
- Organizational unit
- Common name
- Country/Region
- State/Province
- City/Locality

8 Click **Finish**.

The **Security Configuration Progress** page appears.



Managing: wallab-r44150.ca.nortel.com
Security Configuration

Security Configuration Progress

Security server configuration progress:

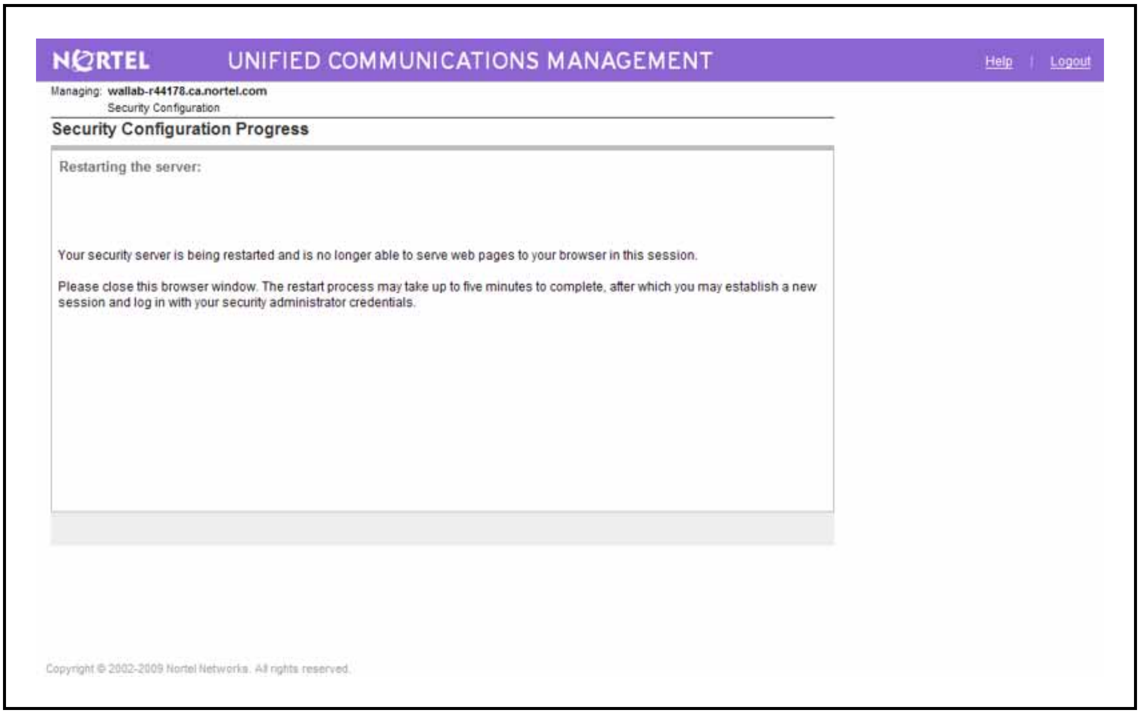
Installing certificate signed by CA: Completed

To complete configuration please click on the Restart button to restart the web server. Wait a few minutes to allow the web server to startup, then login again.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

9 To complete the configuration process, you must restart the web server. Click **Restart**.

The **Security Configuration Progress** page confirms that the server is restarting.


NORTEL UNIFIED COMMUNICATIONS MANAGEMENT
Help | Logout
Managing: wallab-r44178.ca.nortel.com
Security Configuration

Security Configuration Progress

Restarting the server:

Your security server is being restarted and is no longer able to serve web pages to your browser in this session.

Please close this browser window. The restart process may take up to five minutes to complete, after which you may establish a new session and log in with your security administrator credentials.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

--End--

Redundant systems

Redundant systems can join the Unified Communications Management security domain using the following modes:

- Redundant mode—the joining and leaving of the Unified Communications Management security domain operation is mirrored between the active and inactive cores, where the LD 117 commands must be issued from the active server.
  - — LD 117 command: **`[REGISTER / UNREGISTER] UCMSECURITY [DEVICE / SYSTEM]`**
- Split mode—the joining and leaving of the Unified Communications Management security domain operation is performed independently by the active and inactive cores.
  - — LD 117 commands available on active core: **`[REGISTER / UNREGISTER] UCMSECURITY [SYSTEM / DEVICE]`**

The joining and leaving of the Unified Communications Management security domain operation is mirrored between the active and inactive cores.

— LD 117 commands available on inactive core: `[REGISTER / UNREGISTER] UCMSECURITY DEVICE`

Move an element from one UCM security domain to another

This section contains information about moving an element from one UCM security domain to another UCM security domain. This section contains the following procedures:

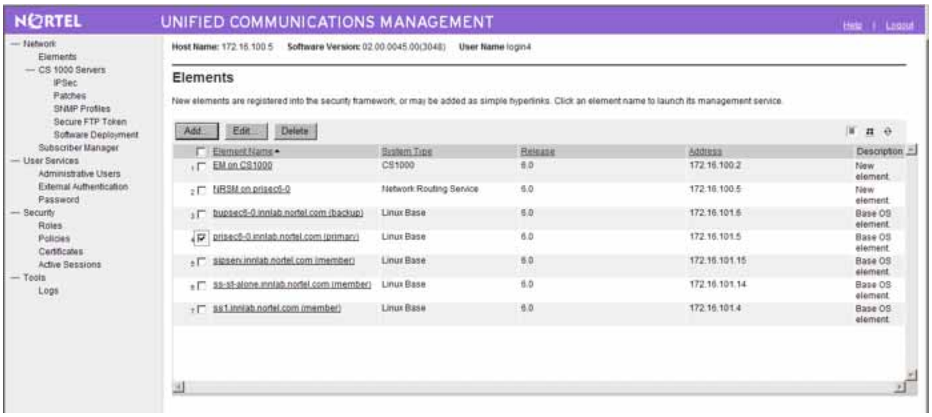
- "Moving a Linux member element to another UCM security domain" (page 267)
- "Moving a single VxWorks element to another UCM security domain" (page 268)
- "Moving all VxWorks elements on a Call Server to another UCM security domain" (page 269)

Moving a Linux member element to another UCM security domain

Perform the steps in this procedure if you are moving a Linux member element from one UCM security domain to another UCM security domain.

Step	Action
1	Log on to the Linux member element using the local login credentials.
2	From the Linux element CLI, perform the appropriate security configuration
3	When prompted, enter the IP address of the new UCM primary security server.
4	Log on to the former UCM primary security server for the Linux element as a user with security administrator privileges.
5	From the navigation tree, click **Elements**. The Elements Web page appears.

Figure 12
Elements Web page in UCM



Host Name: 172.16.100.5 **Software Version:** 02.00.0045.00(3048) **User Name** login4

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service.

	□	Element Name ▲	System Type	Release	Address	Description
1	□	EM on CS1000	CS1000	6.0	172.16.100.2	New element.
2	□	NRSM on prisec6-0	Network Routing Service	6.0	172.16.100.5	New element.
3	□	bupsec6-0.innlab.nortel.com (backup)	Linux Base	6.0	172.16.101.6	Base OS element.
4	☑	prisec6-0.innlab.nortel.com (primary)	Linux Base	6.0	172.16.101.5	Base OS element.
5	□	sipsen.innlab.nortel.com (member)	Linux Base	6.0	172.16.101.15	Base OS element.
6	□	ss-st-alone.innlab.nortel.com (member)	Linux Base	6.0	172.16.101.14	Base OS element.
7	□	ss1.innlab.nortel.com (member)	Linux Base	6.0	172.16.101.4	Base OS element.

6 From the list of elements, select the check box beside the Linux element that has been moved.

7 Click **Delete**.

--End--

Moving a single VxWorks element to another UCM security domain

Follow the steps in this procedure to move a single VxWorks element on a Call Server from one UCM security domain to another.

Step Action

1 On the Call Server, decommission the VxWorks element that is being moved.

2 (Optional) From the element CLI, issue the LD 117 command **`unregister ucmsecurity system`** to remove the device from the UCM security domain.

3 From the element CLI, reconfigure the element using the local setup command.

4 Provision the element on the new Call Server, as required.

5 From the CLI of the device or the CLI of the Call Server, register the element to the UCM security domain by issuing the LD 117 command **`register ucmsecurity system`**.

When prompted, confirm that the element is to be added to the UCM security domain.

6 Log on to the previous UCM primary security server as a user with security administrator privileges.

7 From the navigation tree, click **Elements**.

The Elements Web page appears, as shown in Figure 12 "Elements Web page in UCM" (page 268).

8 From the list of elements, select the check box beside each element that has been moved.

9 Click **Delete**.

--End--

Moving all VxWorks elements on a Call Server to another UCM security domain

Follow the steps in this procedure to move all VxWorks elements on a Call Server from one UCM security domain to another.

Step	Action
1	(Optional) From the Call Server CLI, issue the LD 117 command `unregister ucmsecurity system` to remove all devices registered to the Call Server from the UCM security domain.
2	From the Call Server CLI, issue the LD 117 command `register ucmsecurity system` .
3	Specify the IP address of the new UCM primary security server and the credentials for registering with the UCM security domain.
4	Log on to the previous UCM primary security server as a user with security administrator privileges.
5	From the navigation tree, click **Elements**. The Elements Web page appears, as shown in Figure 12 "Elements Web page in UCM" (page 268).
6	From the list of elements, select the check box beside each element that has been moved.
7	Click **Delete**.

--End--

Authentication methods

The following methods are used for authenticating users and devices on the Communication Server 1000 network.

Central authentication

Unified Communications Management operates at the security domain level and centrally manages and authenticates users and their permissions. When a Communication Server 1000 element joins the UCM security domain, system management and support users log in with accounts defined in UCM, which then authenticates the user based on the password provided and authorizes the functionality that can be accessed based on the permissions that the user has been assigned.

UCM implements role-based access control, which enables a set of permissions to be bundled together into a role. A user obtains permissions to perform various functions by being assigned one or more roles. For information about roles in UCM, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Standalone systems that have not joined the UCM security domain can still use their local authentication and authorization methods. When a Communication Server 1000 Call Server has not joined the security domain, system management and support users log in to the ADMIN, ADMIN2, PDT1, PDT2 and various LAPW accounts. The Call Server locally authenticates the account based on the password provided and authorizes the functionality that can be accessed based on the account permissions. Similarly, when a Communication Server 1000 Signaling Server has not joined the security domain, users log in to the OAM and PDT accounts and the Signaling Server provides local authentication and authorization.

Switch to local authentication

In the event that an element belongs to the UCM security domain and access to the Primary or Secondary UCM Security Server is interrupted, or a device is removed from the security domain, users with network administrator permissions can still access local elements using local authentication and authorization methods.

To reset authentication to local, follow the steps in Procedure 84 “Switching to local authentication” (page 270).

Procedure 84
Switching to local authentication

Step	Action
1	At the device CLI, enter CTRL-P, CTRL-D, CTRL-T to start PDT. Do not enter your UserID at the prompt.
2	At the prompt, enter the authentication reset command: **`resetCAUTH`**

The authentication reset initiates and a message appears stating that you must load the installation media into the removable media drive within 60 seconds.

3 Load the installation media into the removable media drive.

Once the installation media is confirmed, the authentication type is set to LOCAL.

4 Remove the installation media and, if prompted, insert any backup media.

--End--

To rejoin a device to the UCM security domain, you must issue the appropriate command, as described in "Add or remove elements from the UCM security domain" (page 249).

Secure UserID and password authentication with a system security token

A system security token is a randomly generated block of data that generates an algorithm for the creation of a unique password. This password is associated with a specific UserID and is unique to the installation. The data provided by the Unified Communications Management primary security server is used by the system to calculate unique passwords for each of the accounts used by the NFC API (Network File Copy Application Programming Interface), a module contained within the application source code that supplies hardcoded UserIDs and passwords when file transfer requests are made.

The Unified Communications Management primary security server distributes a system-wide security token to elements as they are registered. A security administrator can modify the token from the Unified Communications Management primary security server or schedule the token for modification at periodic intervals. The modified token is then transferred to all registered elements.

The token is transferred to the member servers with best-effort, with attempts made every five minutes until the operation succeeds. The security tokens are transferred using sFTP. If the token on a network element does not match the token distributed by the Unified Communications Management primary security server, sFTP fails.

From the Secure FTP Token Management page in Unified Communications Management, you can refresh the status of the current token or regenerate a new token for distribution throughout the network.

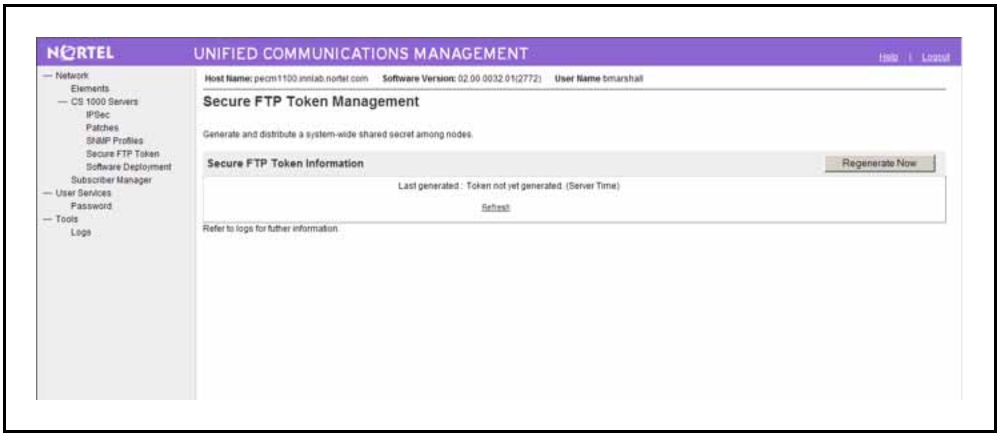
> ***Note:*** The token is backed up during Linux base backup procedures and restored during Linux base upgrades.

Regenerate the Secure FTP Token

Use this procedure to regenerate the Secure FTP token.

Procedure 85
Regenerating the Secure FTP Token

Step	Action
1	Log on to the UCM primary security server.
2	Navigate to **Network > CS 1000 Servers > Secure FTP Token**. The Secure FTP Token Management page appears.



Host Name: pecm1100.innlab.nortel.com **Software Version:** 02.00.0032.01(2772) **User Name** bmarshall

Secure FTP Token Management

Generate and distribute a system-wide shared secret among nodes.

Secure FTP Token Information

Last generated : Token not yet generated. (Server Time)

Refer to logs for futher information.

Step	Action
3	Click **Regenerate Now**.

--End--

Refresh system keys

Several components of the Communication Server 1000 security solution make use of a public key certificate to ensure privacy. These certificates use a digital signature to bind together a public key with an identity, enabling trusted communication without the need for regular exchange of secret keys between endpoints.

To enhance the security of your system, change your system keys periodically. Nortel also recommends that you change your keys (and system passwords) if you have a personnel change and someone who has top-level access to the system leaves your company, or if you fear that system security is compromised in some other way. This applies to all the keys listed in Table 55 "System keys that must be manually refreshed" (page 273).

Table 55
System keys that must be manually refreshed

Key	For more information see:
SSH	"Manage SSH keys using overlays" (page 291) or "SSH key management using Element Manager" (page 296)
ISSS	"Other ISSS configuration and maintenance procedures" (page 87) *Unified Communications Management Common Services Fundamentals* (NN43001-116)
TLS	SIP TLS can use the same key as Element Manager. See *Element Manager System Reference — Administration* (NN43001-632)
sFTP token	"Secure UserID and password authentication with a system security token" (page 271)
Web SSL (HTTPS)	*Element Manager System Reference — Administration* (NN43001-632)
N-Way redundancy	*Network Routing Service Fundamentals* (NN43001-130)

When you refresh the SSH keys, SSH is unavailable until the new keys are generated. On most systems, this occurs almost instantaneously.

Control access to system Application Processors

Restrict access to Application Processors by requiring a user to enter a valid user name and password on the Application Processor console. The user can then access and run applications, or configure operating characteristics of the Application Processor.

System access privileges are based on user IDs that are password-prote cted. Application Processors are UNIX System V-based self-contained modules that interface with the system, and can also interface to local and remote peripheral devices such as terminals, personal computers, and printers. The system restricts or allows access based on user ID, not by the terminal. A user can log on from any terminal, including the system console.

These UNIX-based Application Processors use a hierarchy of four basic user identifications, where number 1 is the highest and number 4 is the lowest. These user IDs are as follows:

- **root**

  First-level user ID used by authorized engineering and development personnel only. The installation routine creates the root user ID, based on the ID of the system to which it is connected. The root ID is different for each application.

- **disttech**

  Second-level user ID used by qualified field technicians, emergency technical assistance and service, and distributors to configure the Application Processor according to the customer applications requirements. disttech is also the second-level default password. The administrator must change this password before placing the system in service.

- **maint** or **mlusr**

  Third-level user IDs used by the customer application and maintenance administrator to install, modify, and remove applications running on the Application Processor. These are also the third-level default passwords.

- **mlusr** and **ccrusr**

  Application access user IDs and fourth-level user IDs used by the application user to access the Application Processor console, local or remote terminals, and personal computers to run applications. These are also the fourth-level default passwords. ccrusr is present only if CCR is installed.

To protect the Application Processor facilities from unauthorized access, see “Recommended password management practices” (page 52).

Configure Secure File Transfer Protocol

Use the procedures in this section to configure Secure Shell (SSH) Secure File Transfer Protocol (sFTP).

> **WARNING**
> sFTP is enabled by default. Do not disable sFTP unless it is required for troubleshooting purposes. sFTP must remain enabled to ensure the successful operation of Communication Server 1000 systems.

sFTP configuration using overlays

Use the following LD 117 commands to configure sFTP on the Call Server.

Table 56
LD117 commands for enabling and disabling secure transport

Command	Preconditions	Description
ENL TRANSFERS INSECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands	• The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0089, indicating insecure transfer is enabled.

Command	Preconditions	Description
ENL TRANSFERS SECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands	• The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0087, indicating the host [host/subnet] is removed from the list of allowed hosts for SSH connection.
DIS TRANSFERS INSECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands • Secure transport has not been disabled. Insecure and secure transports cannot be disabled simultaneously.	• The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0090, indicating that insecure transfer is disabled.
DIS TRANSFERS SECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands • Secure transport has not been disabled. Insecure and secure transports cannot be disabled simultaneously.	• The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0088, indicating secure transfer is disabled.
STAT TRANSFERS INSECURE	None	Displays the insecure transport status
STAT TRANSFERS SECURE	None	Displays the secure transport status

System elements, such as Signaling Server, MGC, and ITG-SA, have access to their local shell commands to enable or disable the secure or insecure transfers, as well as the stat commands. There is no limitation for the execution of stat commands in different shells. However, the enable and disable commands are only provided on the OAM and PDT2 shells and only users with PWD2 rights can execute them.

Table 57
OAM and PDT2 shell commands for enabling and disabling secure transport

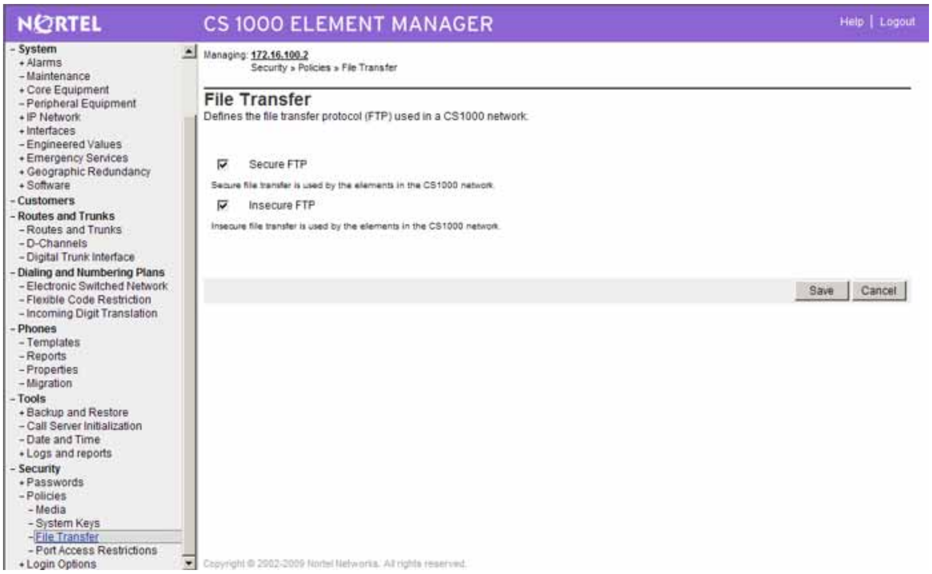
Command	Preconditions	Description
disInsecureTransfers	PWD2 privilege	Disables all insecure FTP transfers in the system.
enlInsecureTransfers	PWD2 privilege	Enables all insecure FTP transfers in the system.
disSecureTransfers	PWD2 privilege	Disables all insecure sFTP transfers in the system.
enlSecureTransfers	PWD2 privilege	Enables all insecure sFTP transfers in the system.
statInsecureTransfers	PWD2 privilege	Displays whether insecure transfer access is enabled or disabled.
statSecureTransfers	PWD2 privilege	Displays whether secure transfer access is enabled or disabled.

sFTP configuration using Element Manger

Use this procedure to configure sFTP using Element Manager.

Procedure 86
Configuring file transfer options using Element Manager

Step	Action
1	Log on to Element Manager as a user with security administrator privileges.
2	Navigate to **Security > Policies > File Transfer**. The File Transfer page displays. By default, the **Secure FTP** and **Insecure FTP** boxes are both selected.



Managing: 172.16.100.2
Security » Policies » File Transfer

File Transfer

Defines the file transfer protocol (FTP) used in a CS1000 network.

☑ Secure FTP

Secure file transfer is used by the elements in the CS1000 network.

☑ Insecure FTP

Insecure file transfer is used by the elements in the CS1000 network.

3 Select or deselect the desired file transfer option. At least one option must be selected or an error message appears.

4 Click **Save**.

You can also click **Cancel** to discard the changes.

> ***Note:*** If you make changes to the file transfer options, you must wait at least 5 minutes before attempting to modify the settings again. Otherwise, an error message appears.

--End--

Configure port access restrictions

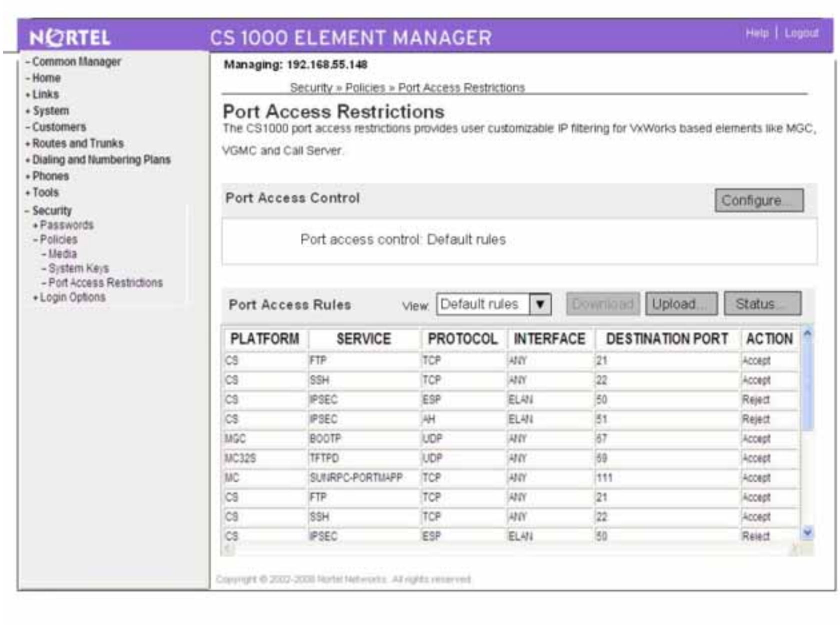
This section provides information about configuring port access restrictions using overlays or Element Manager.

Port Access Restrictions configuration page

You can use Element Manager to configure port access restrictions. To view the port access restrictions details, log on as a user with Security Administrator permissions and navigate to **Security > Policies > Port Access Restrictions**.

The Port Access Restrictions page is shown inFigure 13 "Port Access Restrictions page in Element Manager" (page 278) with the Default rules selected.

Figure 13
Port Access Restrictions page in Element Manager



Managing: 192.168.55.148

Security » Policies » Port Access Restrictions

Port Access Restrictions

The CS1000 port access restrictions provides user customizable IP filtering for VxWorks based elements like MGC, VGMC and Call Server.

Port Access Control

Port access control: Default rules

Port Access Rules

PLATFORM	SERVICE	PROTOCOL	INTERFACE	DESTINATION PORT	ACTION
CS	FTP	TCP	ANY	21	Accept
CS	SSH	TCP	ANY	22	Accept
CS	IPSEC	ESP	ELAN	50	Reject
CS	IPSEC	AH	ELAN	51	Reject
MGC	BOOTP	UDP	ANY	67	Accept
MC32S	TFTPD	UDP	ANY	69	Accept
MC	SUNRPC-PORTMAPP	TCP	ANY	111	Accept
CS	FTP	TCP	ANY	21	Accept
CS	SSH	TCP	ANY	22	Accept
CS	IPSEC	ESP	ELAN	50	Reject

Copyright © 2002-2008 Nortel Networks. All rights reserved.

The Port Access Restrictions page has two main sections:

- Port Access Control—this section indicates whether the current access restriction rules are configured as Default, Custom, or None.
- Port Access Rules—this section displays the current access restriction rules.

From this page you can do the following tasks:

- Configure port access rules
- View the current rules status
- Upload a custom rules file
- Download a custom rules file (this option is only available if a custom rules XML file exists)

For procedures related to port access restrictions and Element Manager, see “Configure port access restrictions using Element Manager” (page 280).

Backing up and restoring port access restrictions

To save changes to the port access restrictions configuration settings, you must perform a data dump on the Call Server. The state of the port blocker (off, default, custom) is also saved when a data dump is performed on the Call Server. The default rules file does not get data dumped because it is installed during upgrade.

You can only backup or restore the custom rules file.

System wide administration commands in LD 117

The following system wide administration commands are available in LD 117. All port access commands require that you have SEC_ADMIN user role privileges.

Table 58
Access restrictions system wide administration commands in LD 117

Command	Description
PORT ACCESS CUSTOM	This command loads the custom port access rules that were uploaded using Element Manager or by FTP. If a custom file exists, the following prompt displays on the console: `Enabling a CUSTOM file could possibly have detrimental effects to the system. Are you sure you want to continue this process? (Yes/[No])` Respond yes to accept the change or no to deny it. If you respond yes, the system verifies the custom file is valid before attempting to load the rules. If the file fails to load, the state will be set back to its previous. If the custom file loads successfully, the Call Server sends a custom state message to all MGC, MC32S, and any inactive Call Server core endpoints to download the files (if necessary) and change their configuration to custom. A datadump is required to save the state.
PORT ACCESS DEFAULT	This command loads the default port access rules stored in a file during installation. If other port access rules are active, those rules are deactivated first. If the default rule file activates successfully, the state on the Call Server changes to default. The Call Server sends a default state message to all MGC, MC32S, and any inactive Call Server core endpoints to download the file (if necessary) and change their configuration to default. A datadump is required to save the state.

Command	Description
PORT ACCESS OFF	This command disables access restrictions on the Call Server and sends an off state message to all MGC, MC32S, and any inactive Call Server core endpoints to change their configuration to off. A datadump is required to save the state.
PORT ACCESS STATUS [ALL / DEBUG]	This command displays the global state of the Access Restrictions. If the DEBUG option is selected, it will also show default and custom signatures with the global status. If the ALL option is selected, it polls the endpoints to detect the local status and lists all cards that do not have matching file signatures or cannot be contacted. If all cards match, a message states that all endpoints match will be displayed.
PORT ACCESS VALIDATE	This command validates a custom file, prints out any errors detected, and provides possible fixes.
PORT ACCESS SHOW DEFAULT	This command displays the rules of the default file in tabular format.
PORT ACCESS SHOW CUSTOM	This command displays the rules of the custom file in tabular format.

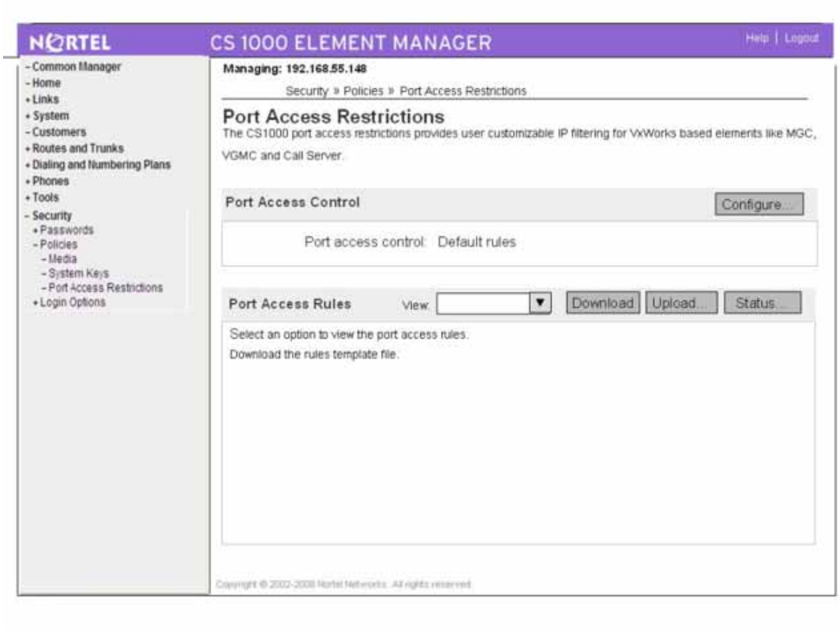
Configure port access restrictions using Element Manager

This section provides information about configuring port access restrictions using the Element Manager interface.

Procedure 87
Configuring port access restrictions using Element Manager

Step	Action
1	Log on to Element Manager as a user with Security Administrator privileges.
2	Navigate to **Security > Policies > Port Access Restrictions**. The Port Access Restrictions Web page appears, as shown in Figure 14 "Element Manager Port Access Restrictions Web page" (page 281).

Figure 14
Element Manager Port Access Restrictions Web page



Managing: 192.168.55.148

Port Access Restrictions

The CS1000 port access restrictions provides user customizable IP filtering for VxWorks based elements like MGC, VGMC and Call Server.

Port Access Control

Port access control: Default rules

Port Access Rules

Select an option to view the port access rules.

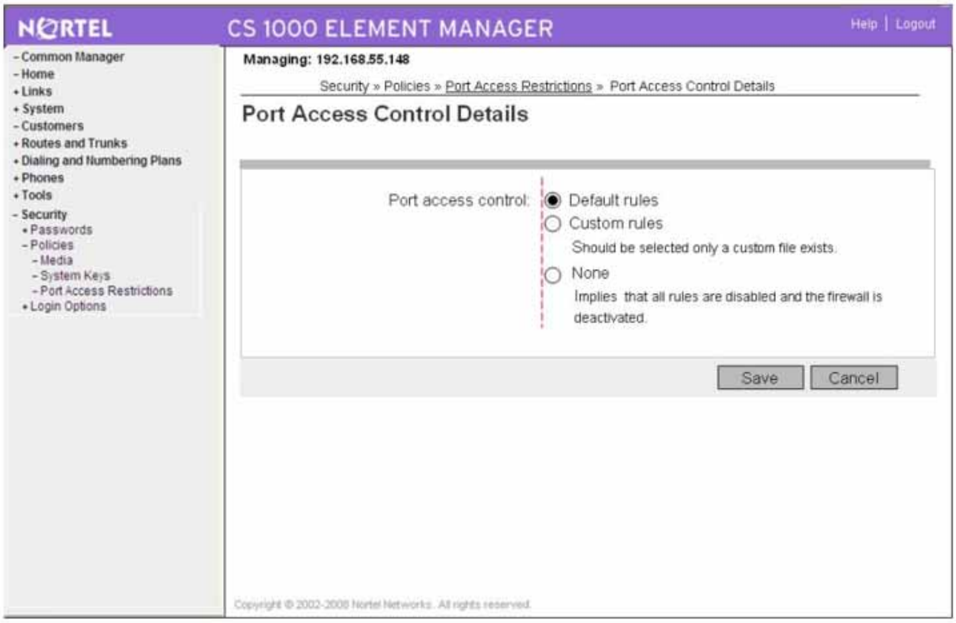
Download the rules template file.

Copyright © 2002-2008 Nortel Networks. All rights reserved.

3 Click **Configure**.

The Port Access Control Details page appears, as shown in Figure 15 "Element Manager Port Access Control Details page" (page 282).

Figure 15
Element Manager Port Access Control Details page



Managing: 192.168.55.148

Security » Policies » Port Access Restrictions » Port Access Control Details

Port Access Control Details

Port access control: ● Default rules
○ Custom rules
Should be selected only a custom file exists.
○ None
Implies that all rules are disabled and the firewall is deactivated.

Copyright © 2002-2008 Nortel Networks. All rights reserved.

4 Select an option from the Port access control rules list. The following options are available:

- Default rules—the system default configurations
- Custom rules—select this option only if a Custom settings file exists
- None—selecting this rule implies that all rules are disabled (except for the mandatory system rules) and that the firewall is deactivated

If you select the Custom rules option, a confirmation message displays. Click **OK** to accept or **Cancel** to return to the list and make another selection.

5 Click **Save**.

You can also click **Cancel** to discard the changes.

--End--

Download the custom rules template file using Element Manager

Use this procedure to download the custom rules template file (template.xml).

Procedure 88
Downloading the custom rules template file using Element Manager

Step	Action
1	Log on to Element Manager as a user with Security Administrator privileges.
2	Navigate to **Security > Policies > Port Access Restrictions**. The Port Access Restrictions page displays.
3	In the Port Access Rules section, verify that the View selection is blank (no selection).
4	Click **Download**.
5	Save the custom rules template file to the local machine. From the browser menu, select **File > Save as**.

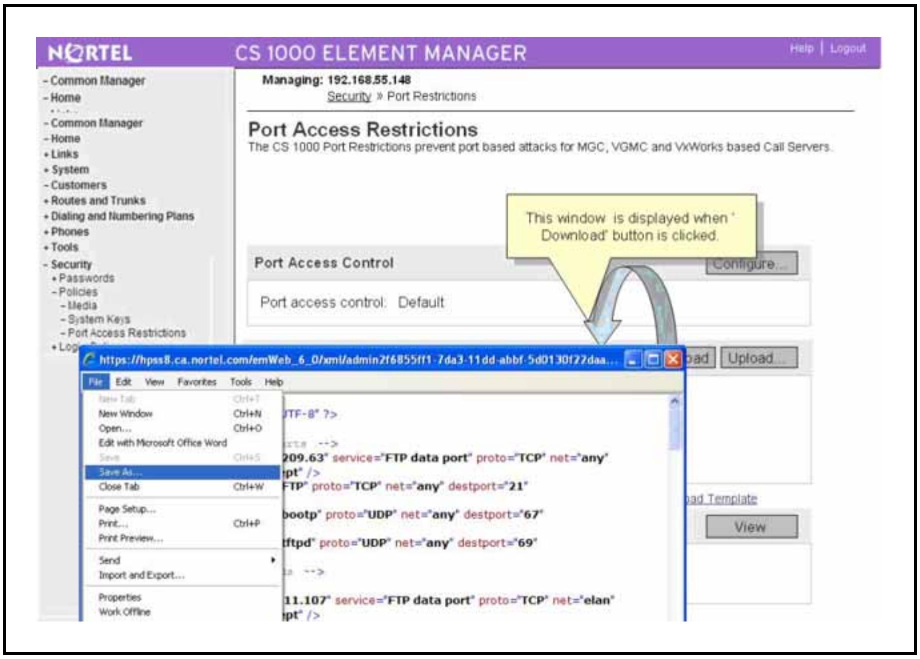
--End--

Download the custom rules file using Element Manager

Use this procedure to download the custom rules file.

Procedure 89
Downloading a custom rules file using Element Manager

Step	Action
1	Log on to Element Manager as a user with Security Administrator privileges.
2	Navigate to **Security > Policies > Port Access Restrictions**. The Port Access Restrictions page displays.
3	In the Port Access Rules section, verify that the View selection is Custom.
4	Click **Download**. A browser window opens displaying the contents of the custom XML file.



Managing: 192.168.55.148

Port Access Restrictions

The CS 1000 Port Restrictions prevent port based attacks for MGC, VGMC and VxWorks based Call Servers.

Port access control: Default

https://hpss8.ca.nortel.com/emWeb_6_0/xml/admin2f6855ff1-7da3-11dd-abbf-5d0130f22daa...

```
TF-8" ?>

rts -->
209.63" service="FTP data port" proto="TCP" net="any"
pt" />
FTP" proto="TCP" net="any" destport="21"

bootp" proto="UDP" net="any" destport="67"

tftpd" proto="UDP" net="any" destport="69"

s -->

11.107" service="FTP data port" proto="TCP" net="elan"
pt" />
```

5 Save the custom file to the local machine. From the browser menu, select **File > Save as**.

--End--

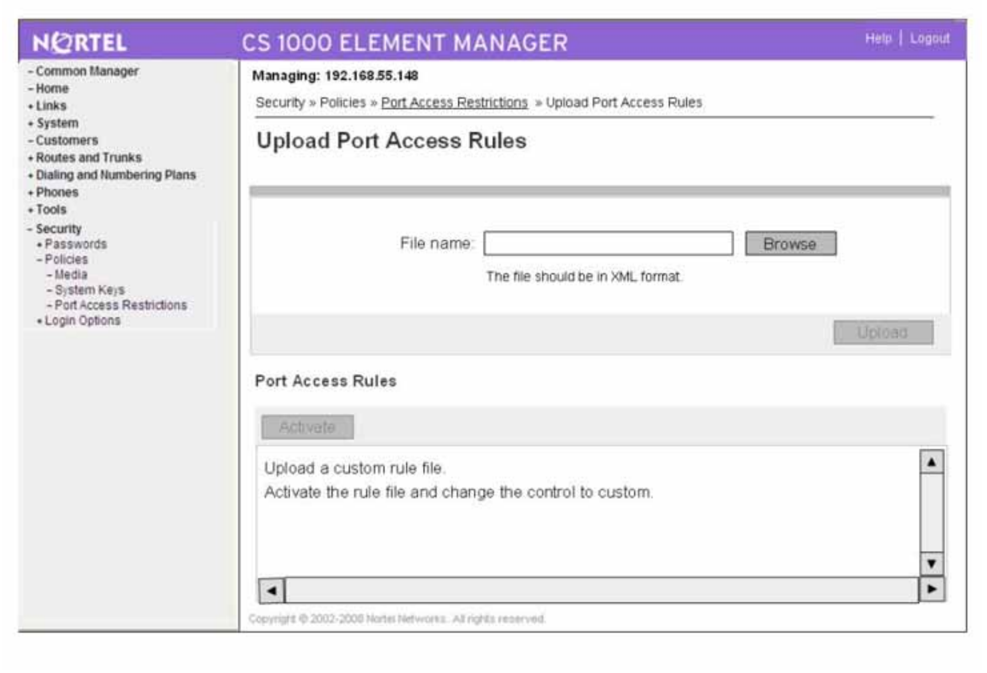
Upload a custom rules file using Element Manager

Use this procedure to upload a customs rule file.

Procedure 90
Uploading a custom rules file using Element Manager

Step	Action
1	Log on to Element Manager as a user with Security Administrator privileges.
2	Navigate to **Security > Policies > Port Access Restrictions**.
3	Click **Upload**.
4	The Upload Port Access Rules page displays, as shown in Figure 16 "Element Manager Upload Port Access Rules page" (page 285).

Figure 16
Element Manager Upload Port Access Rules page



Managing: 192.168.55.148

Upload Port Access Rules

The file should be in XML format.

Upload a custom rule file.
Activate the rule file and change the control to custom.

Copyright © 2002-2008 Nortel Networks. All rights reserved.

5 Click **Browse** to select the custom rules file to upload.

> ***Note:*** The upload file must be in XML format and must have the following filename: customport.xml.

6 Click **OK** to upload the selected file.

If the file is valid, the content of the custom rules file is displayed under the Port Access Rules section and the **Activate** button is enabled.

If the upload fails, or if the file is invalid, an error message displays.

7 Click **Activate**.

The uploaded custom file is activated and the Port Access Restrictions page displays.

--End--

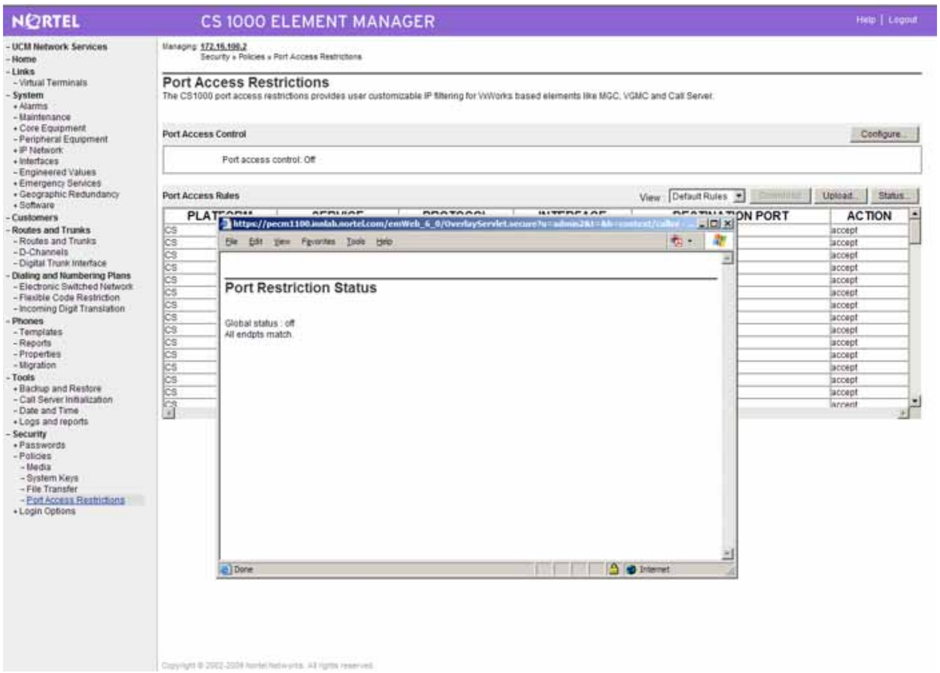
View the port access restrictions status using Element Manager

Use this procedure to view the current port access restrictions status.

Procedure 91
Viewing the port access restrictions status using Element Manager

Step	Action
1	Log on to Element Manager as a user with Security Administrator privileges.
2	Navigate to **Security > Policies > Port Access Restrictions**.
3	Click **Status**. A wait message displays. The status operation can take a few minutes or longer, depending on the number of elements registered to the Call Server. A new window opens and displays the current local and global port access restrictions status, as shown in Figure 17 "Port access restrictions status window" (page 286).

Figure 17
Port access restrictions status window



Managing: 172.16.100.2
Security » Policies » Port Access Restrictions

Port Access Restrictions

The CS1000 port access restrictions provides user customizable IP filtering for VxWorks based elements like MGC, VGMC and Call Server.

Port Access Control

Port access control: Off

Port Access Rules

View: Default Rules

PLATFORM	DESTINATION PORT	ACTION
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept
CS		accept

https://pecm1100.innlab.nortel.com/emWeb_6_0/OverlayServlet.secure?u=admin2&t=&b=context/caller

Port Restriction Status

Global status : off
All endpts match.

Copyright © 2002-2009 Nortel Networks. All rights reserved.

--End--

Configure remote access

This section provides information about configuring Remote Access using overlays or Element Manager.

Manage secure shell access from the Call Server using overlays

Use the following procedure to enable or disable Secure Shell (SSH) access, or to display the status of secure shell access.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 92
Managing secure shell access by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2	At the LD 117 prompt, type one of the following commands: `ENL SHELLS SECURE` to enable secure shells **OR** `DIS SHELLS SECURE` to disable SSH. **OR** `STAT SHELLS SECURE` to display the status of SSH access.

--End--

For more information about the commands used in this procedure, see Table 59 "Job aid: shell management commands in LD 117" (page 287).

Table 59
Job aid: shell management commands in LD 117

Command	Description
ENL SHELLS SECURE	Use this command to enable secure shells in the system.
DIS SHELLS SECURE	Use this command to disable secure shells in the system.
STAT SHELLS SECURE	Use this command to display whether secure shell access is enabled or disabled.
ENL SHELLS INSECURE	Use this command to enable insecure shells in the system, including Telnet and rlogin sessions.
DIS SHELLS INSECURE	Use this command to disable insecure shells in the system, including Telnet and rlogin sessions.
STAT SHELLS INSECURE	Use this command to display whether insecure shell access is enabled or disabled.

Manage insecure shell access from the Call Server using overlays

Use the following procedure to enable or disable insecure shell access, including rlogin and Telnet, or to display the status of insecure shell access.

For more information about the commands used in this procedure, see Table 59 "Job aid: shell management commands in LD 117" (page 287).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 93
Managing insecure shell access by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2	At the LD 117 prompt, type one of the following commands: `ENL SHELLS INSECURE` to enable insecure shells. **OR** `DIS SHELLS INSECURE` to disable insecure shells. **OR** `STAT SHELLS INSECURE` to display the status of insecure shell access.

--End--

Manage insecure shell access on Signaling Server or Voice Gateway Media Card devices using CLI

Use the command line interface (CLI) commands described in this section to enable or disable insecure shells, including FTP, Telnet, and rlogin access, or to display the status of insecure shells.

For more information about the commands used in this procedure, see Table 60 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 289).

Procedure 94
Managing insecure shell access by using CLI

Step	Action
1	Log on using an account that has Level 2 privilege.

2 At the OAM prompt, enter either:

```
enlInsecureShells
```

OR

```
disInsecureShells
```

OR

```
statInsecureShells
```

For more information about the arguments for this command, see Table 60 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 289).

--End--

Table 60
Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices

Command	Description
disInsecureShells	Use this command to disable all insecure shells in the system. This includes Telnet and rlogin sessions.
enlInsecureShells	Use this command to enable all insecure shells in the system. This includes Telnet and rlogin sessions.
statInsecureShells	Use this command to display the status of the insecure shell access.

Enable or disable shell access using Element Manager

Use the following procedure to check the status of secure or insecure shells using Element Manager, or to enable or disable secure shells or insecure shells.

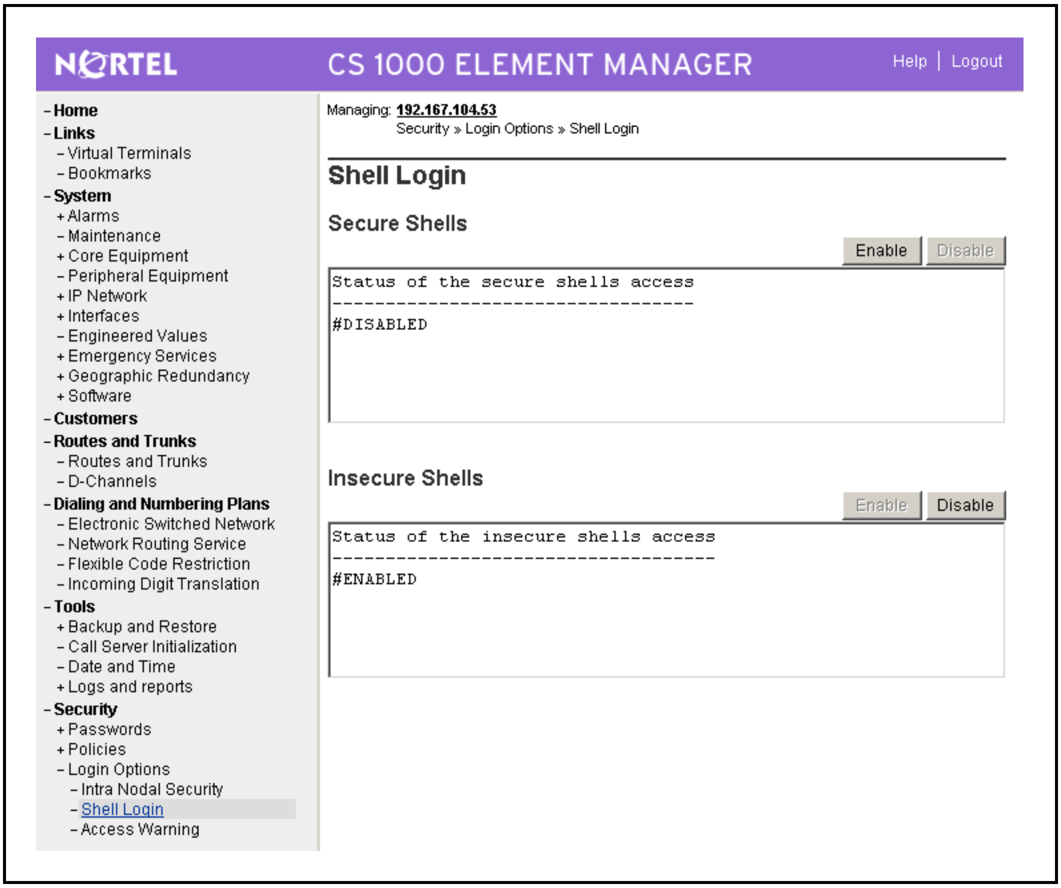
Procedure 95
Enabling or disabling shell access using Element Manager

Step Action

1 Log on to Element Manager using a System password level 2 account.

2 Click **Security > Login Options > Shell Login**.

The status of secure shell access appears in the Secure Shells pane.



Managing: 192.167.104.53
Security » Login Options » Shell Login

Shell Login

Secure Shells

```
Status of the secure shells access
----------------------------------
#DISABLED
```

Insecure Shells

```
Status of the insecure shells access
------------------------------------
#ENABLED
```

3 Click **Enable** or **Disable** to activate or deactivate Secure Shells or Insecure Shells.

--End--

Access the system remotely

SSH, a secure form of rlogin, provides a secure method of logging on remotely. The number of active remote logon shells, including rlogin and SSH sessions, cannot exceed 16 sessions on a system.

To log on remotely using SSH, you must have an SSH client installed on your local system. If your local system runs Microsoft Windows, several SSH clients are available; consult your system administrator to find out what SSH client is installed, and how to use it to log on remotely.

Use the following procedure if your local system runs a UNIX-like operating system (for instance, Linux).

Procedure 96
Log on remotely with SSH using CLI

Step	Action
1	Access the command line interface (CLI) of your operating system.
2	At the operating system command prompt, enter **`$ ssh -l <username> <remote_device_IP>`** A prompt appears requesting a password.
3	Enter the password associated with the user name you entered in the previous step.

--End--

Table 61
Variable definitions

Variable	Value
<username>	A valid user name on the remote device to which you want to log on.
<remote_device_IP>	The IP of the remote device to which you want to log on.

SSH key synchronization between active and inactive cores

To support the joining of standby (inactive) cores to the Unified Communications Management security domain, SSH keys are synchronized between active and inactive cores in redundant systems. The same IP address and SSH key is used for the redundant system, regardless of the core that is active.

Manage SSH keys using overlays

Use the procedures in this section to generate, activate, view, or clear SSH keys using overlays.

Use the following procedure to generate SSH keys from the Call Server.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 97
Generating SSH keys by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.

2 At the LD 117 prompt, enter `SSH KEY GENERATE {ACTIVE|INACTIVE|CABINET [n]}` For more information about the arguments for this command, see Table 62 "Job aid: arguments for SSH KEY GENERATE" (page 292).

When you generate a key, the mutual trust between the device and the Unified Communications Management primary security server is broken until the device rejoins the security domain. A warning message prompts you to do this.

--End--

Table 62
Job aid: arguments for SSH KEY GENERATE

Command argument	Purpose
`SSH KEY GENERATE`	Generates the active SSH keys in the active core. After the key generation, the key is synchronized with the inactive core.
`SSH KEY GENERATE ACTIVE`	Generates the active SSH keys in the active core. After the key generation, the key is synchronized with the inactive core.
`SSH KEY GENERATE INACTIVE`	Generates the active SSH keys in the inactive core. After the key generation, the key is synchronized with the active core.
`SSH KEY GENERATE CABINET [n]`	To generate a key on the MG1000E. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

Use the following procedure to activate SSH keys from the Call Server.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 98
Activating SSH keys by using LD 117

Step	Action

1 Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.

2 At the LD 117 prompt, enter `SSH KEY ACTIVATE {ACTIVE|INACTIVE|CABINET [n]}` For more information about the arguments for this command, see Table 63 "Job aid: arguments for SSH KEY ACTIVATE" (page 293).

--End--

Table 63
Job aid: arguments for SSH KEY ACTIVATE

Command argument	Purpose
`SSH KEY ACTIVATE`	To activate the pending key by restarting the SSH server on the Call Server.
`SSH KEY ACTIVATE ACTIVE`	To activate the pending key by restarting the SSH server on the active core in a two-CPU system.
`SSH KEY ACTIVATE INACTIVE`	To activate the pending key by restarting the SSH server on the inactive core in a two-CPU system.
`SSH KEY ACTIVATE CABINET [n]`	To activate the pending key by restarting the SSH server on the expansion cabinet or MG1000E. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

Use the following procedure to view SSH keys from the Call Server.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 99
Viewing SSH keys by using LD 117

Step	Action
1	Log on to the Call Server CLI.
2	At the LD 117 prompt, enter **`SSH KEY SHOW {ACTIVE|INACTIVE|CABINET [n]}`** For more information about the arguments for this command, see Table 64 "Job aid: arguments for SSH KEY SHOW" (page 293).

--End--

Table 64
Job aid: arguments for SSH KEY SHOW

Command argument	Purpose
`SSH KEY SHOW`	To display the SSH key fingerprint for the active (ENBL) and inactive (STDBY) cores.
`SSH KEY SHOW ACTIVE`	To display the SSH key fingerprint for the active (ENBL) core.
`SSH KEY SHOW INACTIVE`	To display the SSH key fingerprint for the inactive (STDBY) core.

Use the following procedure to clear SSH keys from the Call Server. You must disable secure shells before you can clear SSH keys. For the procedure to disable secure shells, see Procedure 92 “Managing secure shell access by using LD 117” (page 287).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 100
Clearing SSH keys by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2	At the LD 117 prompt, enter **SSH KEY CLEAR {ACTIVE|INACTIVE|CABINET [n]}** For more information about the arguments for this command, see Table 65 "Job aid: arguments for SSH KEY CLEAR" (page 294).

--End--

Table 65
Job aid: arguments for SSH KEY CLEAR

Command argument	Purpose
`SSH KEY CLEAR`	To clear SSH keys stored in the active and inactive cores.
`SSH KEY CLEAR ACTIVE`	To clear the SSH key for the active core. The SSH key stored in the inactive core is removed during the key synchronization process.
`SSH KEY CLEAR INACTIVE`	To clear the SSH key for the inactive core. The SSH key stored in the active core is removed during the key synchronization process.
`SSH KEY CLEAR CABINET [n]`	To clear all of the public keys (active as well as pending) stored on the expansion cabinet or MG1000E system. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

Manage SSH keys using CLI

Use the procedures in this section to generate, view, or clear SSH keys from the OAM, PDT, or IPL prompt.

Use the following procedure to generate SSH keys by using CLI.

Procedure 101
Generating SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the Call Server CLI using a PDT2 account.
2	At the OAM, PDT, or IPL prompt, enter **`SSH KEY GENERATE`** to generate the key on the Call Server, Media Gateway Controller (MGC), or Voice Gateway Media Card.

--End--

Use the following procedure to activate SSH keys by using CLI.

Procedure 102
Activating SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the Call Server CLI using a PDT2 account.
2	At the OAM, PDT, or IPL prompt, enter **`sshKeyActivate`** to activate the pending key by restarting the SSH server on the Call Server, MGC, or Voice Gateway Media Card.

--End--

Use the following procedure to view SSH keys by using CLI.

Procedure 103
Viewing SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the Call Server CLI.
2	At the OAM, PDT, or IPL prompt, enter **`SSH KEY SHOW`** to display the fingerprint of the public key of the Call Server, MGC, or Voice Gateway Media Card. Displays both active and pending keys.

--End--

Use the following procedure to clear SSH keys by using CLI.

Prerequisites

- You must disable secure shells before you can clear SSH keys.

Procedure 104
Clearing SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the Call Server CLI using a PDT2 account.
2	At the OAM, PDT, or IPL prompt, enter `SSH KEY CLEAR` to clear all of the public keys (active as well as pending) stored on the Call Server, MGC, or Voice Gateway Media Card.

--End--

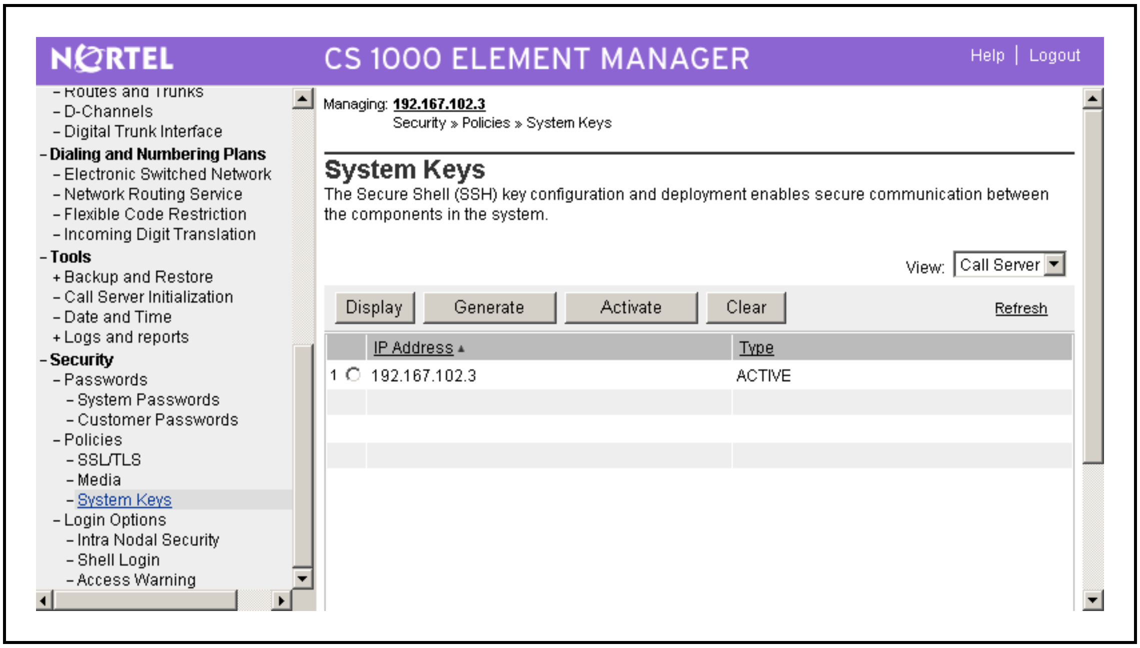
SSH key management using Element Manager

In Element Manager, you can use the System Keys page to display, generate, activate, or clear Secure Shell (SSH) keys for the Call Server, IP Media Gateway (IPMG), and Voice Gateway Media Card.

Procedure 105
Managing SSH keys by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Policies > System Keys** .

The **System Keys** page appears.



Managing: **192.167.102.3**
Security » Policies » System Keys

System Keys

The Secure Shell (SSH) key configuration and deployment enables secure communication between the components in the system.

View: Call Server

	IP Address	Type
1 ○	192.167.102.3	ACTIVE

Step	Action
3	Use the **View** list to select one of:

- **Call Server**
- **IPMG**
- **SS/Voice Gateway Media Card**

The data table displays a list of existing keys in the category you selected. You can sort the columns in the data table by clicking on the column heading.

4 Select the radio button next to the entry you want to edit or view.

5 Either:

Click **Display**
The System Key fingerprint information is appears the System Response pane.

OR

Click **Clear**
The System key information is cleared, and the system response appears in the System Response pane.

OR

Click **Generate**
The System key information is generated, and the system response appears in the System Response pane.

OR

Click **Activate**
The System key information is activated, and the system response appears in the System Response pane.

--End--

Customize the logon banner

The following restrictions apply to the contents of the banner.txt file:

- The file must have the string banner.txt on the first line of the file.
- The file can contain up to 20 lines of text, with up to 80 characters per line.
- The banner text must contain only the following characters: a-z, A-Z, 0-9,,<.>/?;: [{]} ~!@#$%^&*()_-+=| b).

Manage the custom banner using overlays

Use the procedures in this section to view or change the logon banner, or restore the default logon banner using LD 17.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 106
Viewing the banner by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2	At the LD 117 `=>` prompt, enter **`BANNER SHOW`** . The current banner text appears.

--End--

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 107
Loading a new banner by using LD 117

Step	Action
1	Using a program that allows you to send and receive files, log on to the Call Server using a PDT account.
2	Download the file **`banner.txt`** from the directory `/u/pub/` on the Call Server.
3	Using an ASCII text editor, open the **`banner.txt`** file you downloaded in the previous step.
4	Edit the text in the file.
5	Save the file as `banner.txt` in the `/u/pub/` directory on the Call Server.
6	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
7	At the LD 117 `=>` prompt, enter **`BANNER LOAD`**. The contents of the new banner file are loaded.

--End--

These changes are distributed to all Voice Gateway Media Card, MGC and IPMG devices the next time an Equipment Data Dump (EDD) takes place, usually within 24 hours. To force an immediate EDD, see “Force an EDD using overlays” (page 301).

Use the following procedure to restore the default text to the logon banner. Table 10 "Default text of the customizable logon banner" (page 50) shows the default text.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 108
Restoring the default banner by using LD 117

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2	At the LD 117 `=>` prompt, enter **`BANNER RESET`**. The default logon banner text is restored.

--End--

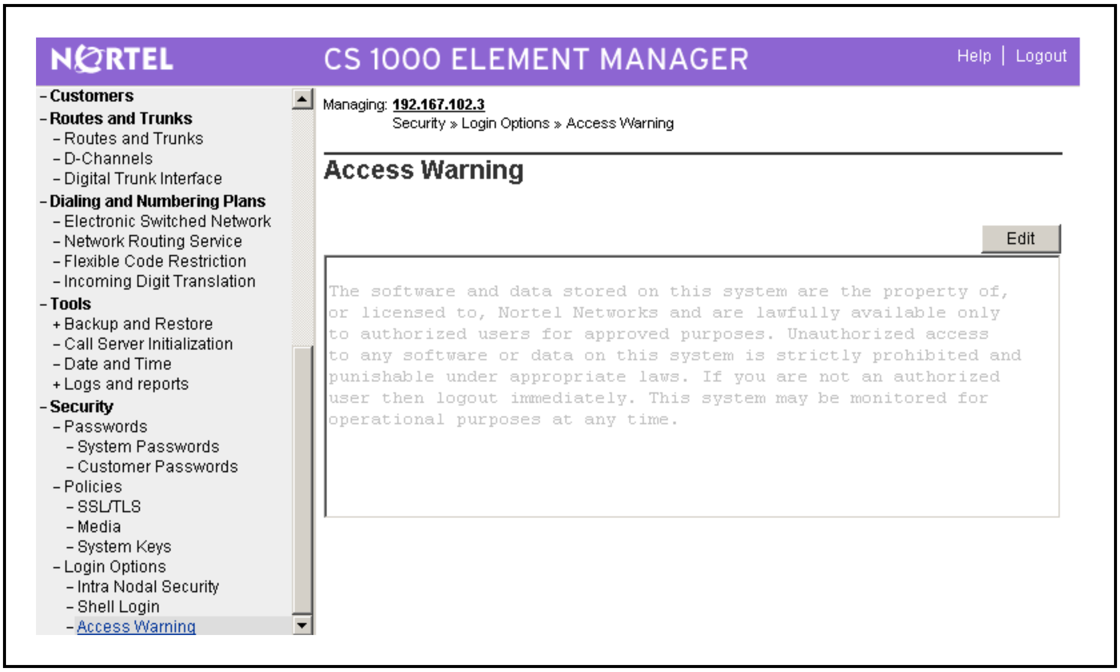
These changes are distributed to all Voice Gateway Media Card, MGC and IPMG devices the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see “Force an EDD using overlays” (page 301).

Manage the custom logon banner using Element Manager

Use the procedures in this section to view or change the logon banner, or restore the default logon banner using Element Manager.

Procedure 109
Viewing or editing the custom banner text by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Access Warning** . The **Access Warning** page appears.



```
The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
```

3 Click **Edit**.

The Edit Login Banner page appears.

4 Edit the banner text.

5 Click **Save** to save and distribute the new banner file.
A confirmation dialog box appears.

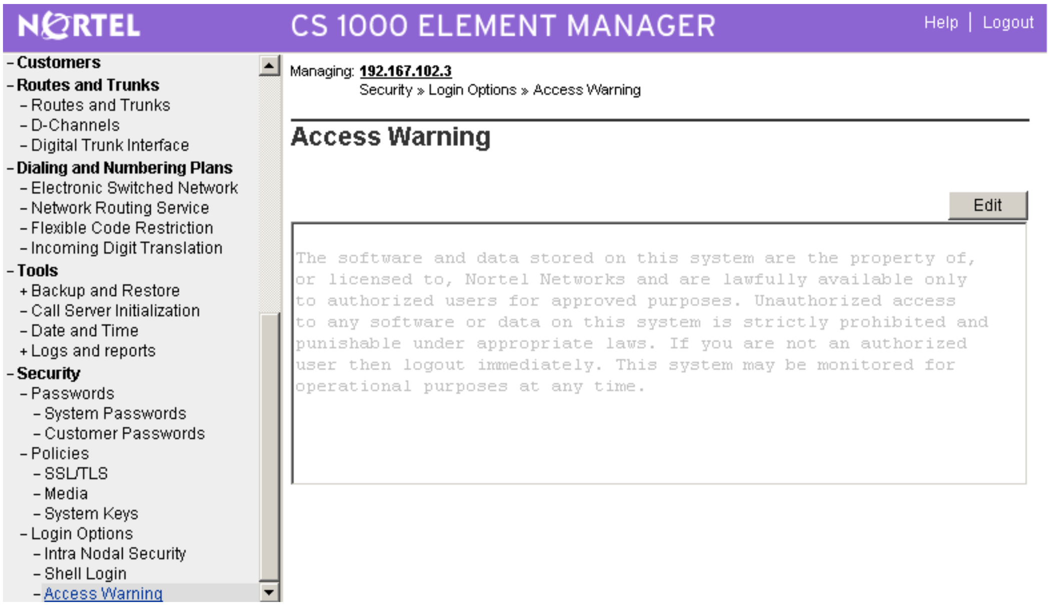
6 Click **OK** to save and distribute the banner file.

--End--

Use the following procedure to restore the default text to the logon banner. Table 10 "Default text of the customizable logon banner" (page 50) shows the default text.

Procedure 110
Restoring the default banner by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Access Warning** . The **Access Warning** page appears.



```
The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
```

3 Click **Edit**.

The Edit Login Banner page appears.

4 Click **Reset**.

--End--

Force an EDD using overlays

Many configuration changes on the system do not take effect until an Equipment Data Dump (EDD) occurs. Use the following procedure to cause the system to perform an immediate EDD, which propagates system changes to all attached devices. An automatic EDD normally occurs at virtual midnight.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 111
Forcing an EDD by using LD 43

Step **Action**

1 Log on to the Call Server CLI using a PWD2 account.

2 At the LD 43 prompt, enter `EDD`. The banner is updated on all peripheral devices (Signaling Server, IPMG, Voice Gateway Media Card, and Inactive Core).

--End--

ATTENTION
System changes and files such as those related to account information and the logon banner are also distributed to all attached devices whenever the system is restarted.

Security debugging

This chapter provides information and procedures to help you perform debugging of security features.

Debug tools are not required during normal operation of the Communication Server 1000 system.

Media Security debug tools

Media Security debug tools are provided to debug system problems, such as voice quality problems or echo.

The Media Security feature establishes cryptographic contexts for securing media packets between endpoints. The system protects the media stream by encrypting media packet payloads and authenticating both payloads and the headers. To avoid compromising this security, debug tools for Media Security are only available in a separate debug mode, and the debug mode can be enabled only by a user that has Account Administrator privilege. When enabling debug mode, you can enable it only on specified terminals, which leaves the rest of the terminals in the system secure. Further, the debug mode is turned off after a configurable period of time.

Enable or disable Media Security debug mode

The Media Security debug mode is disabled by default. Use the following procedure to enable Media Security using commands in LD 80, and to control how long it remains enabled.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 112
Enabling Media Security debug mode by using LD 80

Step	Action
1	Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.

2 At the LD 80 prompt, enter **`EMSD <user-name> <time-out>`** to grant the specified user access to the Media Security debug mode for terminals, nodes, and bandwidth management zones.

For more information about the arguments for this command, see Table 66 "Job aid: arguments for the EMSD command" (page 304).

The Media Security debug key appears in the form of a 64 bit hex value. The key is unique to the current debug session, and is not stored by the system. You must manually record the key if you want to access debug files after the debug session has ended.

--End--

Table 66
Job aid: arguments for the EMSD command

Command Argument	Description
<user-name>	Enter the PDT2 user name to which you want to grant debug access. Only one account can have this permission at any point in time.
<time-out>	Enter the period of time after which the Media Security debug mode is disabled on all terminals, and the system returns to normal operation. Configurable in hours and minutes: <time-out> = <XXX XX> = hours minutes. The default time is 003 00 (3 hours). Configurable in 1 minute intervals to a maximum of 240 00 (10 days).
Example: **`EMSD norteluser 024 00`**. Use this command to enable Media Security debug mode for the user name norteluser, for a period of 24 hours.	

Use the following procedure to manually disable access to the Media Security debug mode.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 113
Disabling Media Security debug mode by using LD 80

Step	Action
1	Log on to the Call Server CLI using an account that has PDT2 privilege.

2	At the LD 80 prompt, enter `CMSD`.

--End--

View information about Media Security debug

Use the following procedure to view information about the Media Security debug mode, including:

- the name of the user account currently assigned Media Security debug privilege
- the time and date when the mode was last enabled or disabled
- the current status (enabled or disabled)
- the time remaining before Media Security debug mode is automatically disabled

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 114
Viewing information about Media Security debug mode by using LD 80

Step	Action
1	Log on to the Call Server CLI using an account that has PDT2 privilege.
2	At the LD 80 prompt, enter `PMSD`.

--End--

Use the following procedure to view information about the Media Security debug mode key used for file encryption. The key is printed in hex format (a 64 bit key is represented in 16 hex characters). Old keys are overwritten and destroyed, so the key that this procedure displays is the one used in the current Media Security debug mode session.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Procedure 115
Viewing information about the current Media Security debug mode key by using LD 80

Step	Action
1	Log on to the Call Server CLI using an account that has PDT2 privilege.
2	At the LD 80 prompt, enter `KMSD`. The key appears. If Media Security debug mode is not enabled, an error message appears.

--End--

Use Media Security Debug

Media Security debug mode offers two modes of operation, as described in Table 67 "Media Security debug modes of operation" (page 306).

Table 67
Media Security debug modes of operation

Debug mode	Description
Media Security override in debug mode for specific terminals	Use this mode to disable media encryption for specific selected terminals, nodes and bandwidth management zone. Enable this option to cause the selected endpoints to transmit unencrypted media. All other terminals operate normally.
Media Security enabled in debug mode for specific terminals	Use this mode to decrypt the traffic between specified terminals. Enable this option to cause the media stream for the selected terminals, nodes, and bandwidth management zone to be encrypted using dynamically generated keys. The keys are stored in a file, and you can use them to decrypt the encrypted media stream.

Use the following four commands to enable or disable Media Security debug mode on specific terminals:

- secDebugOverrideEnable
- secDebugOverrideDisable
- secDebugEnable
- secDebugDisable

To get help for any of these commands, enter them without arguments at the PDT prompt. For more information about how to enable or disable Media Security debug mode, see “Media Security override in Debug mode for specific terminals” (page 307).

Media Security override in Debug mode for specific terminals

Use the following procedures to enable or disable Media Security override in Debug mode for specific terminals using the command line interface (CLI). Enabling this feature temporarily turns off encryption on specified terminals; a timer controls the amount of time before Media Security resumes normal function. The specified terminals continue to operate normally.

Procedure 116
Enabling Media Security override in Debug mode for specific terminals by using CLI

Step	Action
1	Log on to the Call Server CLI using an account that has PDT2 privilege.
2	Access the PDT prompt by holding down the **`ctrl`** key, and typing **`pdt`**. The PDT prompt appears.

3	At the PDT prompt, enter either:
	`secDebugOverrideEnable tn <TN_range_start> <TN_range_end> [<time-out>]`
	OR
	`secDebugOverrideEnable dn <DN_range_start> <DN_range_end> [<time-out>]`
	OR
	`secDebugOverrideEnable node <node_range_start> <node_range_end>`
	OR
	`secDebugOverrideEnable zone <zone_range_start> <zone_range_end> [<time-out>]`

--End--

Table 68
Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to enable debug mode.
<node_range_start> <node_range_end>	The range of nodes for which to enable debug mode.

Table 68
Variable definitions (cont'd.)

Variable	Value
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to enable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to enable debug mode.

Procedure 117
Disabling Media Security override in Debug Mode for specific terminals by using CLI

Step **Action**

1 Log on to the Call Server CLI using an account that has PDT2 privilege.

2 At the PDT2 prompt, enter either:

```
secDebugOverrideDisable tn <TN_range_start>
<TN_range_end>
```

OR

```
secDebugOverrideDisable dn <DN_range_start>
<DN_range_end>
```

OR

```
secDebugOverrideDisable node <node_range_start>
<node_range_end>
```

OR

```
secDebugOverrideDisable zone <zone_range_start>
<zone_range_end>
```

--End--

Table 69
Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to disable debug mode.
<node_range_start> <node_range_end>	The range of nodes for which to disable debug mode.

Table 69
Variable definitions (cont’d.)

Variable	Value
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to disable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to disable debug mode.

Media Security enabled in Debug Mode for specific terminals

Use the information in this section to debug Media Security by decrypting traffic packets between specified terminals, while continuing to use encryption for the media traffic. This approach limits access to the media stream to users who possess the dynamically generated key. Terminals placed in this mode continue to operate normally.

A timer controls the amount of time before Media Security resumes normal function.

Use the following procedures to enable or disable Media Security enabled in Debug Mode for specific terminals.

Procedure 118
Enabling Media Security enabled in Debug Mode for specific terminals by using CLI

Step **Action**

1 Log on to the Call Server CLI using an account that has PDT2 privilege.

2 At the PDT2 prompt, enter either:

```
secDebugEnable tn <TN_range_start> <TN_range_end>
[mode]
```

OR

```
secDebugEnable dn <DN_range_start> <DN_range_end>
[mode]
```

OR

```
secDebugEnable node <node_range_start>
<node_range_end> [mode]
```

OR

```
secDebugEnable zone <zone_range_start>
<zone_range_end> [mode]
```

--End--

Table 70
Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to enable debug mode.
[mode]	
<node_range_start> <node_range_end>	The range of nodes for which to enable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to enable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to enable debug mode.

Procedure 119
Disabling Media Security enabled in Debug Mode for specific terminals by using CLI

Step **Action**

1 Log on to the Call Server CLI using an account that has PDT2 privilege.

2 At the PDT2 prompt, enter either:

```
secDebugDisable tn <TN_range_start> <TN_range_e
nd>
```

OR

```
secDebugDisable dn <DN_range_start> <DN_range_e
nd>
```

OR

```
secDebugDisable node <node_range_start>
<node_range_end>
```

OR

```
secDebugDisable zone <zone_range_start>
<zone_range_end>
```

For more information about the arguments for this command, see Table 71 "Variable definitions" (page 311).

--End--

Table 71
Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to disable debug mode.
<node_range_start> <node_range_end>	The range of nodes for which to disable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to disable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to disable debug mode.

View information about Media Security Debug

Use the following procedure to view the following information:

- all terminals, nodes and zones that have Media Security debug mode enabled
- the time remaining before Media Security debug mode is automatically disabled on each terminal, node, and zone
- the hard drive, file location, and file size for the msdmXXX.log

Procedure 120
Viewing information about Media Security debug by using CLI

Step	Action
1	Log on to the Call Server CLI using an account that has PDT2 privilege.
2	At the PDT2 prompt, enter `secDebugPrintAll`.

--End--

IPsec debug tools

Use the information in this section to debug IP Security (IPsec).

> **ATTENTION**
> When ISSS is enabled and active and you plan to remove a Communication Server 1000 system element, you must first decommission IPsec on the device, or you will be unable to reinstall the device elsewhere. To decommission IPsec locally, use the steps in Procedure 121 “Decommissioning IPsec locally by using CLI” (page 312)

Use the following procedure to decommission IPsec locally on a Voice Gateway Media Card, Media Gateway Controller, or Signaling Server.

Procedure 121
Decommissioning IPsec locally by using CLI

Step	Action
1	Log on to the OAM, PDT, or IPL CLI of the device you want to decommission, using an account that has PWD2 and PDT2 privileges.
2	Enter `isecDecom`.
3	At the confirmation prompt, enter `yes` to remove all IPsec related configuration information from files and memory locally and shut down all related tasks.

--End--

Use the following procedure to view information about IPsec using the OAM, PDT, or IPL prompt.

Procedure 122
Viewing IPsec profile information by using CLI

Step	Action
	Use the following command only if ISSS has been enabled on the element for at least 10-30 seconds. Otherwise, an error may occur.
1	Log on to the OAM, PDT, or IPL CLI of the device you want to view information about.
2	Enter `isecProfileShow`. All IPsec profile information appears.

--End--

Each device must have the same IPsec preshared key (PSK) as the Call Server, and be configured with the same IPsec system security status and level. Use the following procedure to compare the IPsec configuration and IPsec PSK used on the active Call Server with that used on other devices in the system.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing **Enter**.

Use the following procedure to view connection information for IPsec.

Procedure 123
Viewing IPsec connection information by using CLI

Step	Action
1	Log on to the OAM, PDT, or IPL CLI of the device you want to view information about.
2	Enter `isecIkeShowPAll`. For each session, the following information appears: • Source address • Destination address • Initiator/Responder status • Authentication method • Diffie-Hellman group (DH) • Hard lifetime • Encryption algorithm • Hash algorithm

--End--

Use the following procedure to view information about the IPsec network interface.

Procedure 124
Viewing IPsec network interface information by using CLI

Step	Action
1	Log on to the OAM, PDT, or IPL CLI of the device you want to view information about.
2	Enter `isecIPsecShowIf`.

For each session, the following information appears:

- Interface name
- IP address
- DF bit status

--End--

Security logs and alarms

This chapter provides information about operational measurements (OM), logs, alarms, and diagnostic features for security features that have changed or are new in Communication Server 1000 Release 6.0.

For information about messages, logs, and alarms, including System Report (SRPTxxxx) messages, Security Alarms (SECAxxxx), and Security Notification Monitor (SECxxxx) messages, see *Software Input Output Reference — System Messages* (NN43001-712).

This chapter is divided into the following sections:

- “Media Security OMs on Signaling Server” (page 316)
- “OAM Security OMs” (page 317)
- “TLS logs and alarms” (page 317)
- “OAM Transaction Audit and Security Event logging” (page 319)

Media Security OMs

Use the information in this section to access Media Security OMs.

Traffic measurement

Traffic measurements are part of the IP Traffic Report (report 16) and are used to track progress of calls that use Media Security. The following items are tracked:

- calls completed with Media Security <ccms>
- calls completed without Media Security <ccnms>
- calls failed by near end policy <cfnp>
- calls failed by incoming release <cffr>
- outgoing calls switched to RTP <cosr>

- incoming call switched to RTP <cisr>
- calls failed due to lack of resources (not enough Digital Signal Processors (DSP) capable of Secure Real-Time Protocol (SRTP) communication) <cfnr>

You can access these traffic measurements using the **`invs 16`** command, in LD 2, as shown in Table 72 "LD 2: Using invs 16 to access OMs" (page 316).

Table 72
LD 2: Using invs 16 to access OMs

Prompt	Response	Description
.	invs 16	Print expanded Media Security IP Statistics traffic report 16
	OUTPUT	
zone 1 Intrazone	`<cmi><cbi><pi><ai><vi><cmip><cul><cupl><cuj><cur><cuerl><cwl><cwj><cwpl><cwr><cwerl><ccms><ccnms><cfnp><cffr><cosr><cisr><cfnr>`	
Interzone	`<cmo><cbo><po><ao><vo><cmip><cul><cupl><cuj><cur><cuerl><cwl><cwj><cwpl><cwr><cwerl><ccms><ccnms><cfnp><cffr><cosr><cisr><cfnr>`	

Media Security OMs on Signaling Server

The Signaling Server Session Initiation Protocol (SIP) Gateway key management application maintains the Media Security Operational Measurements (OM) listed in Table 73 "Media Security OMs" (page 316)

Table 73
Media Security OMs

OM	Description
SIPVtrkInMSecCallAttempt	Number of secure call origination attempts
SIPVtrkInMSecCallComp	Number of secure call termination attempts
SIPVtrkInMSecErr	Number of secure call originations that have an error in forming the Session Description Protocol (SDP)
SIPVtrkOutMSecCallAttempt	Number of secure call originations completed
SIPVtrkOutMSecCallComp	Number of secure call terminations completed
SIPVtrkOutMSecErr	Number of incoming calls that have incorrect cryptography parameter in the SDP
SIPVtrkMSecCertAuthErr	Number of the certificate authentication failure for Media Security key management

OAM Security OMs

Use the information in this section to access operations, administration, and maintenance (OAM) Security OMs.

Default password change warning

When the default password change warning message appears, the system generates a SEC0029 message to record the event of the warning message, and records it in a log file (/u/rpt/rpt.log) and in a Simple Network Management Protocol (SNMP) trap.

Warning message for Force Password Change

When the default password change warning message appears, the system generates an SRPT195 message to record the event of the warning message, and records the message in a log file (/u/rpt/rpt.log) and in an SNMP trap.

The format of the SRPT195 message is as follows:

```
SRPT195 Force Password Change Activated
```

Example

The following example shows the SRPT195 event log.

```
pdt> rdtail
RPT: ...rd :  95 new reports arrived since last command
RPT: ...rd :  showing 16 records up to the newest record
(rec 435)
...
435 :(1/4/04 16:13:13.570) SRPT195 FORCE PASSWORD
CHANGE ACTIVATED
```

TLS logs and alarms

Table 74 "SIP TLS OMs" (page 317) shows the operational measurements (OMs) relating to Transport Layer Security for Session Initiation Protocol (SIP TLS) that are logged by the SIP Gateway.

Table 74
SIP TLS OMs

OM	Description
SIPVtrkTlsAuthenticationFailure	Number of failed authentication attempts
SIPVtrkTlsIncomingAttempt	Number of incoming SIP TLS connection attempts
SIPVtrkTlsIncomingComp	Number of incoming SIP TLS connection attempts that succeeded
SIPVtrkTlsIncomingFailure	Number of incoming SIP TLS connections that failed

SIPVtrkTlsOutgoingAttempt	Number of outgoing SIP TLS connection attempts
SIPVtrkTlsOutgoingComp	Number of outgoing SIP TLS connection attempts that succeeded
SIPVtrkTlsOutgoingFailure	Number of outgoing SIP TLS connections that failed

Element Manager logs the following OMs related to SIP TLS management:

- change of Secure Socket Layer (SSL) or TLS port number
- change in SSL/TLS Usage setting
- change in Accept Self-Signed Server Certificate setting
- change in Require Client Certificate setting
- change in Allow Redirection from SIPS to SIP setting

Table 75 "SIP TLS alarms" (page 318) shows the alarms relating to TLS that appear on the Signaling Server console as ERROR system logs (syslogs).

Table 75
SIP TLS alarms

Alarm	Description
ITG0113	This alarm indicates a SIP Gateway (GW) TLS initialization failure (severity level: major). This covers conditions such as a failure to read TLS parameters from the configuration file, certificate not found, or certificate invalid.
SEC0001	This alarm indicates that the number of SIP GW TLS connection failures for a remote IP exceeded the threshold (severity level: major). The initial value of the threshold is 3 failures within 30 minutes from the same remote IP address. The cause of the last failure is indicated in the reason code.

Every day at virtual midnight, the system checks for impending certificate expiry. If any certificate in the system is within 21 days of expiration, the following alarm is generated: `Certificate to expire within x days (severity level: major).`

The system generates a log, and optional alarm, whenever any of the following events occur:

- turn SSL ON or OFF
- import certificates
- assign certificates
- delete certificates
- renew existing certificates
- create a new certificate

sFTP security alarms

Table 76 "Security alarms related to sFTP" (page 319) shows alarms related to Secure File Transport Protocol.

Table 76
Security alarms related to sFTP

Alarm	Description
SEC0087	Secure transfers are enabled. Applications can transfer data based on secure transfer protocols, such as sFTP. This is an informational message; no action is required.
SEC0088	Secure transfers are disabled. Applications cannot transfer data based on secure transfer protocols, such as sFTP. This is an informational message; no action is required.
SEC0089	Insecure transfers are enabled. Applications can transfer data based on insecure transfer protocols, such as FTP. This is an informational message; no action is required.
SEC0090	Insecure transfers are disabled. Applications cannot transfer data based on insecure transfer protocols, such as FTP. This is an informational message; no action is required.

OAM Transaction Audit and Security Event logging

Security audit logs must contain sufficient information for after-the-fact investigation or analysis of security incidents. These audit logs provide a means for accomplishing several security-related objectives including individual accountability, reconstruction of past events, intrusion detection, and problem analysis.

The OAM Transaction Audit Logging feature on Communication Server 1000 maintains an audit trail of all system administrator OAM activities that have taken place on Unified Communications Management User Interfaces. This feature provides the OAM logs only for Communication Server 1000 management applications running on a Linux platform. The OAM log records include operational, configuration and maintenance events of Communication Server 1000 management applications.

For more information about OAM Transaction Audit logging, see the Communication Server 1000 logging section of *System Management Reference* (NN43001-600).

Security Event log

The security.log file is stored in the “/var/log/nortel/OAM” directory of the Unified Communications Management Primary Security server. OAM Transaction Audit and Security Event Logging consolidates all Communication Server 1000 security events into security.log. This log file contains all of the security-related events generated by Communication Server 1000 management applications installed on Linux platforms. These audit log files have a log rotation of 30 days.

Examples of security-related events include:

- Security policy changes
- Logon success and failures
- Certificate changes
- User Account Creation and Illegal (failed) Login Events
- Any OAM security event where security administrator privilege (or flag) is enabled or required

Security administrators can view the security logs by accessing the log viewer interface, which is found by navigating to **Tools > Logs** on the Unified Communications Management primary security server.

For more information about Security Event logging, see the Communication Server 1000 logging section of *System Management Reference* (NN43001-600).

Appendix A: Standards

This appendix provides information about the Communication Server 1000 system compliance with various security standards. The appendix is divided into the following sections:

- “Media Security FIPS conformance” (page 321)
- “Encryption technology” (page 322)

Media Security FIPS conformance

The Media Security feature conforms to FIPS 140-2 cryptographic standard Security Level 2. A government and industry working group composed of both operators and vendors developed the FIPS 140-2 standard. The FIPS 140-2 standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. The FIPS 140-2 standard specifies four security levels for cryptographic modules, which provides a wide spectrum of options according to data sensitivity. The Media Security feature conforms to Level 2. Security Level 1 and 2 are described as follows:

- Security Level 1 is the lowest level of security for a cryptographic module. It permits the operations of the software and firmware components on a general purpose computing system using an unevaluated operating system. The operating system is not required to have physical security mechanisms beyond the basic requirements for production grade components, but must have at least one approved algorithm or approved security function.
- Security Level 2 enhances the physical security mechanisms of Security Level 1 by adding requirements for tamper-evidence, which includes the use of temper-evident coating or seals or for pick-resistant locks on removable covers or doors of the module.

  Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform the corresponding services.

Security Level 2 permits the operation of the software components of the cryptographic module on a general purpose computing system. The operating system must meet the functional requirements specified in the Common Criteria (CC) Protection Profiles (PP), Annex B of FIPS 140-2 specification. The operating system must be evaluated at the CC evaluation assurance level EAL2 (or higher).

Encryption technology

Table 77 "Encryption technologies used in CS 1000" (page 322) lists encryption technologies used in Communication Server 1000 Release 5.0 and later.

Table 77
Encryption technologies used in CS 1000

AES	The Advanced Encryption Standard (AES) is a block cipher that is widely accepted as an encryption standard, replacing the Data Encryption Standard (DES).
SHA-256	The Secure Hash Algorithm (SHA) (FIPS 180) protects data from tampering or damage during transmission. SHA-256 is considered more secure that SHA-1.

Encryption technology supported in UNIStim DTLS

UNIStim DTLS uses the Mocana DTLS library stack, which is FIPS certified (FIPS 140-2, Level 1, certificate number #927).

Table 78 "Ciphers supported by Mocana DTLS library" (page 322) lists the ciphers supported by the Mocana DTLS library for UNIStim DTLS in Communication Server 1000 Release 6.0 and later.

Table 78
Ciphers supported by Mocana DTLS library

TLS-RSA-WITH-AES-256-CBC-SHA
TLS-RSA-WITH-AES-128-CBC-SHA
TLS-RSA-WITH-3DES-EDE-CBC-SHA
TLS-RSA-WITH-DES-CBC-SHA
TLS-DHE-RSA-WITH-AES-256-CBC-SHA
TLS-DHE-RSA-WITH-AES-128-CBC-SHA
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA
TLS-DHE-RSA-WITH-DES-CBC-SHA
TLS-DH-ANON-WITH-AES-256-CBC-SHA

TLS-DH-ANON-WITH-AES-128-CBC-SHA
TLS-DH-ANON-WITH-3DES-EDE-CBC-SHA
TLS-DH-ANON-WITH-DES-CBC-SHA
TLS-PSK-WITH-AES-256-CBC-SHA
TLS-PSK-WITH-AES-128-CBC-SHA
TLS-PSK-WITH-3DES-EDE-CBC-SHA
TLS-RSA-PSK-WITH-AES-256-CBC-SHA
TLS-RSA-PSK-WITH-AES-128-CBC-SHA
TLS-RSA-PSK-WITH-3DES-EDE-CBC-SHA
TLS-DHE-PSK-WITH-AES-256-CBC-SHA
TLS-DHE-PSK-WITH-AES-128-CBC-SHA
TLS-DHE-PSK-WITH-3DES-EDE-CBC-SHA
TLS-RSA-WITH-NULL-SHA
TLS-RSA-WITH-NULL-MD5

Table 79 "Advanced encryption technologies supported by Mocana DTLS library" (page 323) lists the advanced encryption technologies supported by the Mocana DTLS library for UNIStim DTLS in Communication Server 1000 Release 6.0 and later.

Table 79
Advanced encryption technologies supported by Mocana DTLS library

Diffie-Hellman key exchange
RSA
PKCS #1, Version 1.5
PKCS #5
PKCS #7
PKCS #8
PKCS #10
PKCS #12
MD2
MD4
MD5
SHA1
SHA-224
SHA-256

SHA-384
SHA-512

Terminology

A

authentication

A process that checks the credentials of a security principal against values in an identity store.

authorization

The process of resolving a user's entitlements with the permissions configured on a resource to control access.

C

certificate

In order to verify the identity of an endpoint, some features of the Communication Server 1000 system use a digital certificate.

Class of Service

Class of Service. You can use Class of Service to create restrictions on calling, such as no outgoing calls or no long distance.

E

EDD

Equipment Data Dump. An EDD propagates system changes to all attached devices. Many configuration changes on the system do not take effect until an EDD takes place. An EDD normally occurs automatically at virtual midnight.

F

fingerprint

In public-key cryptography, a public key fingerprint is used to verify identity.

I

IPsec

The IP Security (IPsec) framework provides intranodal security on the Communication Server 1000 system. IPsec is a standard that can be used to secure internet protocol (IP) communications by encrypting and authenticating IP packets. IPsec provides security at the network layer, and consists of a group of cryptographic protocols for securing packet flows and key exchange. The two packet flows are:

- Encapsulating Security Payload (ESP), which provides authentication, data confidentiality, and message integrity
- Authentication Header (AH), which provides authentication and message integrity, but does not provide confidentiality

IPsec uses the Internet Key Exchange (IKE) protocol.

IPsec operates at Layer 3 (the network layer) of the OSI model. Therefore, IPsec can protect both TCP and UDP-based protocols.

L

LD

(Also Load, Overlay). See Overlay.

leg

A section of the path information traverses in a network. In telephony, a call is described as being broken into several legs if it passes over, for example, a combination of IP and nonIP equipment.

M

MGC

Media Gateway Controller.

MIKEY

In cryptography, a key management protocol.

N

NRS Manager

Network Routing Service Manager. The Network Routing Service (NRS) Manager is a Web interface that you can use to manage the NRS. The NRS Manager application resides on the Signaling Server. The NRS includes both the H.323 Gatekeeper and

Session Initiation Protocol (SIP) Redirect/Registrar Server, and provides routing services to both H.323- and SIP-compliant devices.

O

OAM

(Also OA&M). Operation, Administration, and Management.

OM

An operational measurement report where information about system activity is stored.

Overlay

Overlays are a programming method that software developers can use to create computer programs that are larger than available memory. Each overlay consists of a group of commands, organized by function. Only one overlay is loaded at any time.

P

PEM

Privacy-Enhanced Electronic Mail (PEM) is a proposed Internet Engineering Task Force (IETF) standard that provides cryptographic protection of e-mail messages.

S

SDesc

Security Descriptions

secret

(Also secret key). A secret string that is used to transform information into an encrypted format, and back into a readable format. Some types of encryption use two keys (often called a key pair), where one key is used to encrypt data, and another to decrypt it.

SFTP

Secure File Transfer Protocol. A network protocol that enables the secure exchange of data using SSH standards. See also the entry for SSH.

SHA

(Also SHA-1, SHA-256.) The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions. SHA-1 is the most common of the SHA functions, and appears in a variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPsec. Industry experts consider SHA-256 to be more secure than SHA-1, and often use it to secure critical information. The SHA algorithms are designed by the US government National Security Agency (NSA).

SIP

Session Initiation Protocol (SIP) is a protocol for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. SIP clients traditionally use TCP and UDP port 5060 to connect to SIP endpoints, including SIP servers. Telephony systems use SIP in setting up and tearing down voice or video calls. However, SIP also offers session initiation for applications such as Event Subscription and Notification, Terminal mobility. All voice and video communications are transmitted using Real-time Transport Protocol (RTP).

SRTP

Secure Real-time Transport Protocol (or SRTP) is a secure form of Real-time Transport Protocol (RTP). SRTP provides encryption, authentication, and replay protection, and protects message integrity for RTP data in both unicast and multicast applications. A related protocol, Secure RTCP (SRTCP), provides the same security-related features to RTCP that SRTP provides to RTP.

SSH

Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers .

T

TDM

Time Division Multiplexing.

TLS

Transport Layer Security (TLS), (which replaces Secure Socket Layer [SSL]) is a cryptographic protocol that provides secure communications over the Internet for applications such as e-mail, Internet fax, and other data transfers that require security. In many applications, only the server is authenticated, and the client is unauthenticated. TLS also supports mutual authentication, which requires that a public key infrastructure be deployed to the clients. In either case, TLS protects communication from eavesdropping, tampering, and message forgery.

TN

Terminal Number.

Index

A

access control management 47
access restrictions
- configuration 277

account types 212
add an element 95
administration program security
- access control 216
- audit trail reviews 222
- history file 233

application processor security 273
audit trails
- reviews 222

authcodes
- Level 1 accounts 47

B

backup security server 29
BUG messages 233

C

cable plan records 249
ccrusr user IDs 274
certificate
- add CA to endpoint 100
- assign existing 159
- change trust status 101
- create renew request 148
- CRL Details 166
- delete CA 102
- delete pending 146
- export self-signed 151
- export with key 153
- import with key 156
- install to trusted list 98
- process pending 144
- remove current 163
- replace existing 161
- revoke 165
- SIP TLS
  - self-signed 123, 140
  - third-party CA 129
  - upgrading 134, 138
- view information 105
- Web SSL
  - local CA 107
  - self-signed 117
  - third-party CA 112

certificates
- creating 103
- management 103

CS 1000 and Meridian 1 system access security 247
- administration program access 45
- application processors 273
- network facilities 249
- switchroom 248
- system administration port 248

CSC (customer service change) activities 233
customizable logon banner 49

D

Datagram Transport Layer Security 44
DISA (Direct Inward System Access) security
- Level 1 accounts 47

disabled ports 248
disttech user IDs 273
DTLS 44

F
force EDD 301

H
Hardening 31
  Basic 31
  Enhanced 32
history file 233

I
IDF (Intermediate Distribution Frame) 249
insecure passwords 222
Intrasystem Signaling Security 36
IP Security 36
IPsec 36
ISSS 36, 69
ISSS/IPsec 36
  configuring 69
  configuring manually
    creating a target 90
    ports secured by ISSS 69
  configuring manually using CLI 90
  maintenance on Linux servers 87

K
key generation 23
key management 23
keys 291
  activating 295
  clearing 296
  generating 295
  showing 295

L
LAPW 216
LAPW (Limited Access Password) 47
Level 2 accounts
  administration programs 47
Limited Access Password 216
Limited Access to Overlays 216
Limited Access to Overlays feature 47
lineman test terminals 249
lockout
  override 48
log files
  traffic 233
logon banner 297, 299
  display 298
  edit 299
  load 298
  managing 297
  restore 299–300

M
maint user IDs 274
managing passwords
  reset other passwords 231
  using CLI
    changing PDT password 225
    reset Call Server passwords 228
    stand-alone Signaling Server 233
  using Element Manager 234
    add LAPW user 236
    add user 234
    edit user 239
    global password settings 242
    SSH 289
  using overlays 224
managing users
  using overlays 214
managing users and passwords
  using overlays 214
    account information 220
    privileges 226
MDF (Main Distribution Frame) 249
Media Security 42, 183
  Class of Service 196
  configuring 183, 196, 201
  dependencies 43
  FIPS conformance 321
  security icon 43
  system-wide setting 201
    Element Manager 196
    LD 17 201
mlusr user IDs 274
MSSD 183
MTC (maintenance messages) 233
multi-user log on 231
multi-user login 231

N
network security 249
Nortel Unified Communications Manager 49

P
password hash strengthening 48

password settings 48
passwords
  application processors 273
  port 248
  STA 232
port access restrictions 40
port security 248
primary security server 29, 96
Print Only program restrictions 216
PRT ports 248
public-key certificates 25
  managing 95

R
remote access
  configuration 286
  enable/disable insecure shell 288
  enable/disable SSH 287–288
  logging on remotely 290
role types 49
roles 212
root user IDs 273

S
SCH (service change) activities 233
Secure File Transfer protocol 38
secure remote access 49
secure signaling 42
security administration 49, 247
security debugging 303
security domain manager 30
security server 96
Set Based Administration 216
SFTP 38
  See also Secure File Transfer protocol
Single Terminal Access 232
SIP 169
SIP Proxy
  configuration of SIP TLS 171
SIP TLS 44, 169
  configuring
    config.ini 174
  configuring using Element Manager 175
    security disabled 176, 179
    security policy 176
  diagnostic 181
SIP TLS configuration 171
SSH 49
STA 232
switchroom security 248
system access security 247
  administration program access 45
system administration port security 248
system keys 23

T
time stamps 216
traffic log files 233
TTY ports 248

U
user and password management 209
user ID
  application processors 273
user name
  application processors 273

V
VHST command 233
View private CA details 97
view user accounts 220

Nortel Communication Server 1000

Security Management Fundamentals

Release: 6.0
Publication: NN43001-604
Document revision: 03.08
Document release date: 14 April 2010

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

www.nortel.com