Nortel Communication Server 1000

Security Management Fundamentals

Release: 5.5
Document Revision: 02.09

www.nortel.com

NN43001-604

Nortel Communication Server 1000
Release: 5.5
Publication: NN43001-604
Document release date: 8 January 2009

LEGAL NOTICE

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.

Sourced in Canada

Contents

New in this release

The following change is introduced in *Security Management Fundamentals (NN43001-604)* () for CS 1000 Release 5.5:

- Enterprise Common Manager (ECM) now supports a Release value for entries in the managed elements table.

Other changes

For a detailed history of past releases of this document, see Table 1 "Revision History" (page 9).

Table 1
Revision History

Date	Description
January 2009	Standard 02.09 This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5, and to add information in the section About Media Security.
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.

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

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

- how to create and control user accounts
- how to protect signaling and the media stream from privacy intrusions or disruption
- how to administer and use secure remote access

This document contains information about configuring security features using overlays, Element Manager, and in some cases using command line interfaces (CLI). This document also contains information about using Enterprise Common Manager (ECM) to manage certificates. For information about using ECM to configure security features, and for information about security features available in ECM, see *Enterprise Common Manager 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:

Other security information

This Nortel Technical Publication (NTP) provides information about many of the features you can use to provide security for your CS 1000 system. Some security features are described in other NTPs. For more information, see Table 2 "Other NTPs that contain security information" (page 14).

Table 2
Other NTPs that contain security information

Telephony Services Access Control Management (NN43001-602) ()
Element Manager System Reference — Administration (NN43001-632) ()
Enterprise Common Manager Fundamentals (NN43001-116) ()
IP Phones Fundamentals (NN43001-368) ()
Secure Multimedia Controller Fundamentals (NN43001-325) ()
Network Routing Service Installation and Commissioning (NN43001-564) ()

About this document

This section provides an overview of how you can control unauthorized access and provide security for the system. It describes the reason 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 5.5 software. 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 PII, CP PIV and CP PM
- Communication Server 1000M Single Group (CS 1000M SG) CP PII, CP PIV
- Communication Server 1000M Multi Group (CS 1000M MG) CP PII, CP PIV
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 61C CP PII, CP PIV
- Meridian 1 PBX 81C CP PII, 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 1 "Meridian 1 systems to CS 1000 systems" (page 8) lists each Meridian 1 system that supports an upgrade path to a CS 1000 system.

Table 3
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
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

Intended audience

This document is intended for administrators responsible for configuring 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

The following systems are referred to generically as "Small System":

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as "Large System":

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

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:

For more information about the features described in this chapter, see "Fundamentals of system security management" (page 29).

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 229))
- program access control (see *Telephony Services Access Control Management (NN43001-602)* ())
- Audit Trail review (see "Configure LAPW Audit Trail using overlays" (page 240))
- History File review (see "History File configuration using overlays" (page 250))

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 CS 1000 Release 5.5, user names are required for all log on sessions. If you upgrade from CS 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 4 "User names created when accounts without user names are converted from CS 1000 Release 3.0" (page 19).

CAUTION

If you are upgrading from CS 1000 Release 4.5 or earlier to CS 1000 Release 5.5, 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 5.5, the system prevents you from creating accounts with these reserved names.

Table 4
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:

- Install and configure a Secure Multimedia Controller (SMC) 2450 to protect UNIStim signaling. For more information about SMC 2450, see *Secure Multimedia Controller Fundamentals (NN43001-325)* () .
- 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). Nortel also recommends that you use ISSS/IP security (IPsec) to protect communication between ECM servers (for example, ECM with Element Manager) and CS 1000 system components (for example, call servers and signaling servers).

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 installing an SMC 2450, 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, but can take up to two hours on Time Division Multiplexing (TDM)-only systems that use SSC as the call processor.

Nortel recommends that you use SSH whenever possible, and disable insecure shells (rlogin, and telnet) on the CS 1000 system, except as needed. Both Secure Shell and insecure shells are enabled by default. Table 5 "Examples of cases where insecure shells are required" (page 20) lists some instances where insecure shells are required.

Table 5
Examples of cases where insecure shells are required

Feature or device	Insecure shell required
Virtual terminals on Element Manager	If you plan to use virtual terminals on Element Manager, you must enable insecure shells because Element Manager cannot use SSH.
Net IQ	If you plan to use Net IQ, you must enable insecure shells because Net IQ cannot use SSH.
Telephone 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 CS 1000 system to work with certificates provided by a certificate authority (CA), (which can be either a private certificate authority such as the Nortel Enterprise Common Manager (ECM) 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 (NN43001-106) Book 4 of 6 (I to M)* () .

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 ECM as the primary security server before you install your Linux-based NRS, and configure all of your NRS to be part of the same ECM security domain.

Nortel recommends that you perform certificate management from the same ECM Linux host that is running Element Manager, because you can then enable ISSS on all of the CS 1000 system elements managed from that host. Element Manager on ECM 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 ECM). The system uses the same association to protect certificate management.

If you perform certificate management from an ECM 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 ECM 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 3 "SIP TLS with multiple security domains" (page 194).

Upgrade from an earlier release

The following security administration issues pertain when you upgrade to CS 1000 Release 5.5 from a previous release:

- 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 4.5 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 CS 1000 Release 4.5 to Release 5.5, 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 the upgrading, because it takes time to obtain the certificate.
  To obtain a certificate signed by a public CA, see Procedure 48 “Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading” (page 161), and Procedure 49 “Processing a pending certificate response for SIP TLS when upgrading” (page 165).

Recommendations to protect IP Phones

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

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)* () .

It is particularly important that you enable GARP Ignore on systems where no SMC 2450 is installed to provide UNIStim encryption.

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. For more information about configuring 802.1x authentication, see *IP Phones Fundamentals (NN43001-368)* () .

Security interactions

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

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 6 "Interactions between ISSS and Element Manager web server on Signalling Server" (page 23).

Table 6
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 6
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 131) [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 ECM

If you are using Element Manager on ECM to manage CS 1000 systems, Nortel recommends that you enable ISSS to protect confidentiality of communication between Element Manager and the CS 1000 systems. ISSS is required to protect communication between Element Manager on ECM and the CS 1000 systems because Xmsg protocol is used by Element Manager on ECM to communicate with CS 1000 systems, and Xmsg provides neither encryption nor authentication. You must add the ECM IP addresses as external IPsec targets on the CS 1000 system call server, and configure ISSS/IPsec for the CS 1000 system on ECM; for more information see "First-time configuration and activation of ISSS" (page 48).

ECM supports a unique ISSS/IPsec preshared key (PSK) for each CS 1000 system managed by ECM. In the list of elements managed by ECM, you must enter the IPsec PSK for each managed CS 1000 system, and it must be the same IPsec PSK that you use to configure ISSS on the CS 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 265).

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 7 "ISSS interaction with FTP" (page 25).

Table 7
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.

IPsec also requires that all devices in the IPsec target list use the same preshared key (PSK). Therefore, all of the targets, including the Primary, Secondary, and Alternate Call Servers, must use the same PSK.

ISSS and AML

If you configure ISSS to Full Security, Applications Module Link (AML) connections to CallPilot and Symposium Call Center are still allowed but are not protected unless you define them as IPsec targets. The AML link to the Signalling Server of SIP CTI is protected by IPsec.

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, AML, 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 is required to link to Symposium Call Center and CallPilot, but does not have its own encryption; you can configure ISSS to protect AML. To do so, manually add the device to the target list. For more information about adding an IPsec target manually, see Procedure 20 “Creating an ISSS target by using LD 117” (page 109).

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 8 "Interactions between Media Security and CallPilot on systems without MGC daughterboards or MC32S" (page 27).

Table 8
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 or Small System Controller (SSC) cabinets with MC32S.

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 9 "Consequences of SIP trunk security" (page 27) for an explanation of the consequences of SIP TLS security configuration on Failsafe NRS.

Table 9
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.
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.

Fundamentals of system security management

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

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

- Install and configure a Secure Multimedia Controller (SMC) 2450. For more information about SMC 2450, see *Secure Multimedia Controller Fundamentals (NN43001-325)* () .
- Configure Intrasystem Signaling Security Solution (ISSS) 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 CS 1000 system elements Embedded LAN (ELAN) interface, and over the ECM Linux host ELAN 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.

CS 1000 Release 5.5 includes several system components including a call server, signaling servers, 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:
  - CP Side 0 and CP Side 1 of the CS 1000 logical call server (LCS) with the high availability option
  - Signaling Servers associated with a specific Call Server
  - Voice Gateway Media Cards in collocated IPMGs

  All systems include an ELAN subnet to which the CS 1000 Call server ELAN interface and its collocated system elements connect. The MGC and its media daughterboard exchange control information using the TLAN 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.
- Communication through the TLAN subnet is not protected by ISSS/IPsec. The following are examples of components that connect through their TLAN interfaces to the TLAN subnet:
  - Signaling Servers associated with Alternate Call Server for remote survivable MG 1000E IPMGs
  - n-way redundant Alternate Call Servers for remote survivable MG 1000E IPMGs
  - MGC media daughterboard
  - Voice Gateway Media Cards in IPMGs
  - Geographic Redundancy Secondary or Alternate Call Servers
  - Collocated IP Media Gateway (IPMG) Media Gateway Controllers (MGC)
  - IPMG

In addition to CS 1000 system components, CS 1000 supports Linux-based Network Routing Service (NRS) and Element Manager on Enterprise Common Manager (ECM). NRS or Element Manager can run on ECM servers anywhere within an Enterprise network, even sites that are geographically remote from CS 1000 system components. You can use ISSS/IPsec to protect communication between Element Manager on ECM and ECM Certificate Manager.

System security overview

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

- Platform security
  - 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
  - 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

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 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 211).

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 10 "IP Phones capable of establishing a secure connection using Media Security" (page 32).

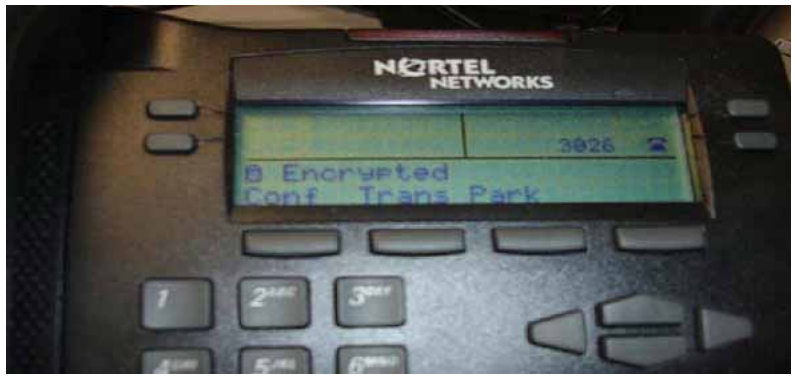
Table 10
IP Phones capable of establishing a secure connection using Media Security

IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E
IP Phone 2007
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 32); 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 193).

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.

General signaling security concepts

This section provides an overview of Intrasystem Signaling Security (ISSS), Secure Multimedia Controller (SMC) 2450, public-key certificates, and NRS SIP Proxy.

ISSS/IPsec

IP Security (IPsec) provides an ISSS solution that works with all IP protocols. For procedures relating to ISSS, see “ISSS” (page 45).

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 is disabled by default. If you want to use ISSS, you must configure it using Overlay 117 or Element Manager.

The default ISSS setting (enabled or disabled) for each target is the same as the system ISSS setting, unless you enable or disable ISSS for the target. If you enable or disable ISSS for a target, the target IP address is stored in an exception list (isec.txt).

You can enable and disable ISSS from the call server. You can also use commands in LD 117 to modify the ISSS settings and propagate those settings to all registered devices.

Secure Multimedia Controller

Secure UNIStim signaling, provided by the transparent UNIStim security proxy within the Secure Multimedia Controller (SMC) 2450, encrypts data exchanges between the Signaling Server and the IP Phones. Secure UNIStim signaling thereby makes it possible for UNIStim IP Phones to

communicate with UNIStim servers in a protected fashion, with encryption terminated at the SMC 2450 before the unencrypted traffic moves to the local server.

To use UNIStim signaling security, you must have an SMC 2450 installed in the system. You can also use the SMC 2450 to create Secure Multimedia Zones (SMZ), which protect the signaling and media infrastructures of the MCS 5100 and CS 1000 product lines. All signaling and media traffic entering or leaving the SMZ must pass through the SMC 2450. For more information about SMC 2450, see *Secure Multimedia Controller Fundamentals (NN43001-325)* () .

Key management concepts

The encryption technology used in CS 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

CS 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 CS 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 CS 1000 system, these new keys are generated automatically, in others you must manually refresh the keys from time to time.

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 are shared using this method.
- preshared between endpoints in the system. You can manually configure preshared keys used by some features. ISSS and Geographic Redundancy keys 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, Enterprise Common Manager (ECM), 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 36).

Public-key certificate concepts

Overview

SSL and TLS protocols are used to provide transportation layer security for web-based HTTP management traffic, 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.

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

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).

Enterprise Common Manager provides a centralized console for managing X.509 certificates, including issuing certificates, distributing certificates to CS 1000 devices (for example, a SIP Gateway), and managing the trusted CA certificate list on CS 1000 devices. For example, from the certificate management console, X.509 certificates can be assigned remotely to Web SSL and SIP TLS services on VxWorks-based SIP Gateways, as well as Linux-based NRS and Element Manager servers. Different services on the same device can have their own certificates, or share a common certificate. For example, Web SSL and SIP TLS services running on the same device can share the same X.509 certificate.

Certificate types

The ECM certificate management console supports three types of certificates:

- Self-signed certificates. Self-signed certificates are issued by themselves, not by a CA. This type of certificate does not provide any authentication, and are vulnerable to man-in-the-middle attack. Nortel recommends that you avoid using self-signed certificates.
- Certificates signed by the private CA hosted on ECM primary security server. During the installation of the ECM 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 ECM 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 of the customer organization (for example, the CA from the customer's IT department) or an outside commercial CA (for example, Verisign or Thawte). You can use the ECM X.509 certificate management console to generate a Certificate Signing Request (CSR) from a target device, and then send the CSR to a public CA to obtain a certificate response, which contains a X.509 certificate. You can use the ECM certificate management console to process the certificate response returned from a public CA, and thereby 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 ECM 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 along a series of certificates, each one verifying that the next 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 SIP Proxy, the number of CA trust certificates installed must be the same as the number of certificates in the chain. However, on SIP GW, you need only install the intermediate CA to the trust list for Verisign and Thawte. For examples of the certificates included in a chain, see Table 11 "Examples of certificates in a chain" (page 38).

Table 11
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

ECM 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 SIP Proxy, but only the intermediate CA certificate for 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 SIP Proxy and SIP Gateway.

To use certificates signed by a third-party CA, you must carry out the following four 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 ECM to manage certificates for both Web SSL endpoints and SSL/TLS endpoints. Use the certificate management tools provided by Enterprise Common Manager (ECM) to import, export, and assign certificates, and to create certificates or certificates requests. To manage certificates by using ECM, you must log on with a user name that has Security Administrator access.

For certificate and CA management procedures, see "Certificate Management" (page 123).

NRS SIP Proxy

SIP Proxy mediates between trusted and nontrusted SIP endpoints. For more information about SIP Proxy, see *Network Routing Service Installation and Commissioning (NN43001-564)* () .

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 229).

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.

System accounts

CS 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 12 "Default user names and passwords" (page 40).

Table 12
Default user names and passwords

	Password				
User Name	**Call Server**	**Signaling Server, Media Gateway Controller, Voice Gateway media Card**	**ECM**	**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

Table 12
Default user names and passwords (cont'd.)

User Name	Password				
	Call Server	Signaling Server, Media Gateway Controller, Voice Gateway media Card	ECM	SMC 2450	NRS Manager
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 13 "Account level descriptions" (page 41).

Table 13
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 50 "Job aid: LD 17 user and password prompts" (page 233). To display a list of all accounts that have insecure passwords, see Procedure 78 “Checking for insecure passwords using LD 22” (page 239).

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 CS 1000 Release 4.5 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 CS 1000 Release 5.0 and later, 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 CS 1000 Release 5.0 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. You must install package 164 LAPW Limited Access to Overlays to use the Default Password Change feature. 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 ECM

Role management facilities are available on the system only if Nortel Enterprise Common Manager (ECM) 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 instance, you can assign individual access to the debugging shell (PDT), or change the access privileges of a whole group of users by modifying one of the roles assigned to them. The role management facility provides the basic role types described in Table 14 "Roles in ECM" (page 43).

Table 14
Roles in ECM

Role name	Description
CS1000_Level1	Full access to overlays and customers.
Debugger	Access to advanced debugging utilities.
LinuxDebug	Access to operating system level debugging utilities from the Linux shell.
NrsmMonitor	Read-only access to NRS elements.

Patcher	Access to software maintenance functions.
PowerUser	Ability to carry out operation, administration, and maintenance on elements.

For more information about role-management and other security features available in ECM, see *Enterprise Common Manager 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 263).

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, which appears when a user logs on to the system. The customizable banner is intended for use by customers that have security policies that require network equipment to display a specific message to users when they log on. 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 15 "Default text of the customizable logon banner" (page 44).

Table 15
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.

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:

For more information about ISSS/IPsec, see "ISSS/IPsec" (page 34).

ATTENTION
Nortel recommends that you install and configure all system components before you configure and enable ISSS. Adding a system component after ISSS is configured and enabled is more complex than adding the same component before ISSS is enabled.

About ISSS

Communication Server 1000 (CS 1000) is a distributed IP telephony system with components (such as Call Server, Signaling Server, and Media Gateway Controllers (MGC)) that you can distribute throughout the Enterprise network. Therefore, signaling is not restricted to the Call Server ELAN subnet and can pass over the Layer 3 Enterprise network. ISSS/IPsec protects the communication between system components and between the management application and system components. ISSS/IPsec works with all IP protocols.

To use ISSS, you must first upgrade all Small System Controllers (SSC) to CP PM for call servers, and to NTDW60 MGC for MG 1000E IP Media Gateways (IPMG). The SSC does not support ISSS, regardless of whether the SSC is functioning as a Call Server or as an IPMG MGC.

ISSS employs IPsec to provide security services, including confidentiality, authentication, and anti-replay, to application layer protocols. CS 1000 provides simplified, automated IPsec policy configuration, and avoids complex configuration requirements inherent in many implementations of IPsec.

In each CS 1000 system, the call server functions as the central control point of ISSS configuration and automatically propagates ISSS configurations to all elements within that CS 1000 system. For example, if you configure ISSS between Element Manager on ECM and the managed CS 1000 system call server, you do not need to configure it between Element Manager on ECM and each element of the managed CS 1000 system.

The ISSS feature uses a preshared key (PSK) for authentication and each CS 1000 uses a common PSK for all elements within the system. Element Manager on ECM can manage multiple CS 1000 systems and can share a unique PSK with each managed CS 1000 system.

CAUTION
When ISSS is configured and enabled, Nortel recommends that you decommission IPsec on any CS 1000 system element before you remove the device. To decommission IPsec locally, use the steps in Procedure 112 “Decommissioning IPsec locally by using CLI” (page 285).

For more information about ISSS/IPsec, see “ISSS/IPsec” (page 34).

ISSS configuration overview

ATTENTION
The following restrictions apply to ISSS/IPsec:

- On VxWorks-based devices, IPsec applies only to the ELAN.
- To use ISSS, you must upgrade all IPMG from SSC to MGC.
- IPsec is not automatically configured on the Linux server. You must configure IPsec on the Linux server after you enable ISSS on the system, otherwise communication between the Linux server and VxWorks-based devices is not possible if the devices are configured to use ISSS security level Full.

To configure ISSS, perform the following tasks:

1. Configure the ISSS parameters and enable ISSS on the CS 1000 Release 5.0 or 5.5 system

   For the procedures you must follow to complete this task, see “Recommended methods for first-time ISSS configuration” (page 49).

— Ensure that all system elements (Signaling Servers, MGCs, and Voice Gateway Media Cards) are registered with the call server so ISSS configuration is automatically transferred from the call server to the elements.
If a system element is not registered with the call server, for example when you add a system element after ISSS is enabled, you must configure ISSS for the new element. For more information, see “Add, remove, or replace a CS 1000 system element when ISSS is enabled and active” (page 68).

— enter a PSK on the call server

— configure the ISSS security level (OPTI, FUNC, or FULL) on the call server. For more information about ISSS security level configuration, see Table 19 "Job aid: ISSS/IPsec security levels" (page 55).

— enable ISSS on the call server

— Commit the changes

2. Configure ISSS on ECM Linux host (if applicable).

   For the procedures you must follow to complete this task, see “Recommended methods for first-time ISSS configuration” (page 49).

   — configure the IPsec PSK and ISSS security level for each IPsec target, which includes, for example, signaling servers on each CS 1000 system

   ATTENTION
   The ISSS security level Full is not available on ECM. If the Call Server is configured to use ISSS security level Full, configure the ECM to use the ISSS security level FUNC. For an illustration of this mapping, see Table 16 "CS 1000 and ECM ISSS security level map" (page 48).

   — If ECM is coresident with Element Manager, then configure ISSS from within Element Manager

   — If ECM is not coresident with Element Manager (or if ECM is coresident with Element Manager, and you want to create an IPsec target pointing to another Linux host) then manually configure IPsec targets using the newipsectarget command. For more information about this command, see Table 24 "Job Aid: Linux shell scripts you can use to configure IPsec on Linux" (page 67).

3. Add or replace CS 1000 system elements after ISSS is enabled and configured.

   For the procedures you must follow to complete this task, see “Add, remove, or replace a CS 1000 system element when ISSS is enabled and active” (page 68).

Table 16
CS 1000 and ECM ISSS security level map

CS 1000 ISSS security level	Corresponding ECM security level
OPTI	OPTI
FUNC	FUNC
FULL	FUNC

First-time configuration and activation of ISSS

Use the procedures in this section to perform initial configuration of ISSS. If you have already configured and enabled ISSS and want to add a component or perform other maintenance, see “Add, remove, or replace a CS 1000 system element when ISSS is enabled and active” (page 68) and “Other ISSS configuration and maintenance procedures” (page 96).

ATTENTION
If your system includes Element Manager on ECM, Nortel recommends that you configure and enable ISSS on the local CS 1000 System before configuring it on remote centralized ECM.

Table 17
Job aid: ISSS/IPsec security levels

ISSS/IPsec security level	Description
Optimized Security	(OPTI) Traffic over pbxLink and Xmsg between this host and its IPsec targets[1]is protected by IPsec. Any other traffic (other than pbxLink or Xmsg) between this host and its IPsec targets is permitted, but is NOT protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.
Functional Security	(FUNC) All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.

Table 17
Job aid: ISSS/IPsec security levels (cont'd.)

Full Security	(FULL)[3] All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is NOT permitted, except BootP, SSH (port 22), SSL (port 443), NTP (port 123), and AML (port 888). To connect with Element Manager on a signaling server over the ELAN when ISSS security policy Full is used, you must use HTTPS (HTTPS uses SSL).
Note[1] IPsec targets are either internal IPsec targets are that are added automatically when certain devices read IP addresses from a system configuration file and create IPsec targets for them, or external IPsec targets that are added from the command line. Note[2] ISSS neither blocks nor encrypts connections through the TLAN subnet. For VxWorks based hosts (Signaling Server, MGC, Voice Gateway Media Card), all traffic over the TLAN subnet is accepted over IP and is not encrypted. Note[3] ISSS security policy FULL is not available on the ECM host. If you configure the CS 1000 System to use ISSS security policy Full, configure the ECM to use ISSS security policy FUNC.	

Recommended methods for first-time ISSS configuration

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.

Use the following procedure to configure and enable ISSS. This procedure also provides the steps necessary to ensure that ISSS/IPsec applies to all XMSG commands sent by Element Manager to each CS 1000 system component.

Part of this procedure involves creating SNMP trap destinations. This causes ELAN routes to be created from each device to Element Manager (these routes are needed for ISSS/IPsec to function), and also sends SNMP traps to Element Manager (for future development).

Prerequisites

- Ensure that all system elements (Signaling Servers, MGCs, and Voice Gateway Media Cards) are registered with the call server.
- Ensure that all MC32S and IPMG devices have their complete image installed, and have been restarted.

Procedure 1
Configuring ISSS for the first time

Step	Action
1	If you have multiple IP telephony nodes in the same CS 1000 system, or if you have a CS 1000E, then you must select a signaling server on which to run Element Manager locally with ISSS enabled. Once you have configured and enabled ISSS/IPsec, you must use Element Manager on this Signaling Server for all system configuration and management. For CS 1000M systems with only one IP Telephony node, proceed to step 15.
2	Log on to the OAM shell on the Signaling Server you selected in step 1, using a PWD2 account.

3	Enter the following command to create an IPsec target:
	isecNewTarget <MGC ELAN 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? (Yes/[No]):`

4	Enter: **yes** The following message appears: `The new target has been added locally.`
5	Repeat steps 2 through 4 for each MGC in the CS 1000E system. If there is only one IP Telephony node associated with the CS 1000 Call Server, proceed to step 15.

6	If there is more than one IP Telephony Node associated with the CS 1000 Call Server, enter the following command to create an IPsec target:
	isecNewTarget <SignalingServer/VGMC ELAN 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?  (Yes/[No]):
```

7 Enter:
yes
The following message appears:
```
The new target has been added locally.
```

8 Repeat steps 6 through 7 for each Signaling Server and Voice Gateway Media Card in each IP Telephony Node, except for those in the same IP Telephony Node as the Signaling Server you selected in step 1.

9 Log on to the command line of an MGC in the CS 1000E system.

10 Enter the following command to create a target pointing back to the ELAN interface of the Signaling Server you selected in Step 1:
isecNewTarget <local Element Manager ELAN IP>

11 Repeat step 9 and 10 for each MGC in the CS 1000E system.

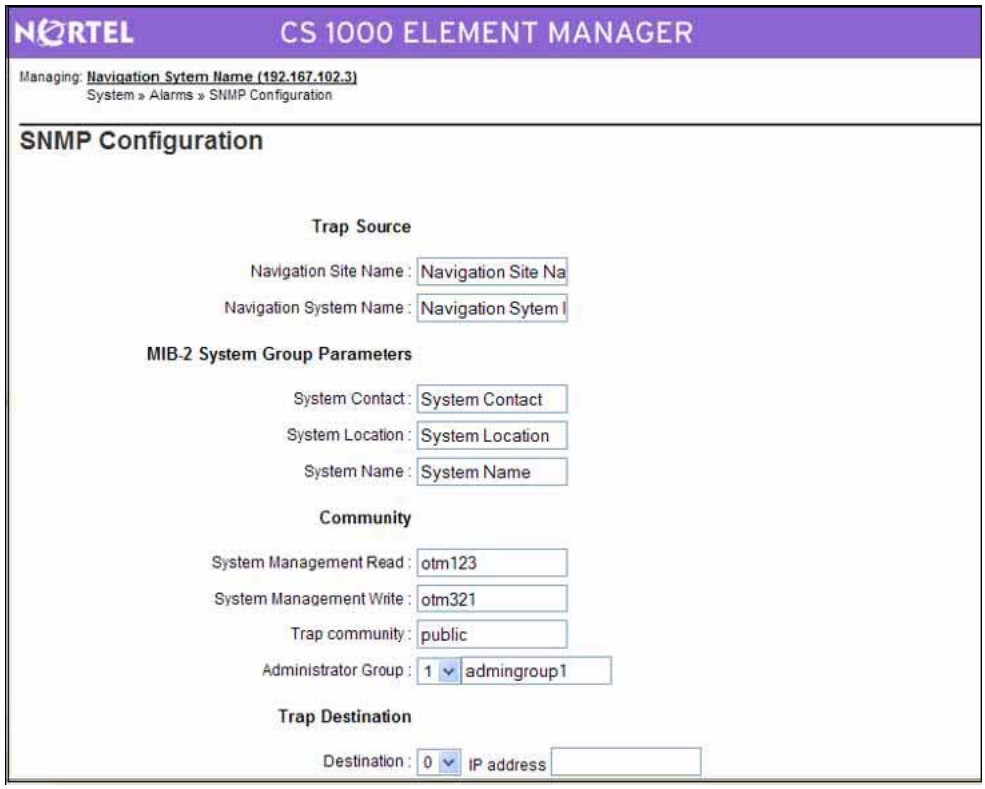
12 Log on to the command line of one of the Signaling Servers or Voice Gateway Media Cards that you targeted in Step 6.

13 Enter the following command to create a target pointing back to the ELAN interface of the Signaling Server you selected in Step 1:
isecNewTarget <local Element Manager ELAN IP>

14 Repeat step 12 and 13 for each MGC in the CS 1000E system.

15 Log on to Element Manager on the local Signaling Server using a System password level 2 account.

16 Click **System** > **Alarms** > **SNMP**.
The **SNMP Configuration** page appears.



17 In the **Destination** field, select a trap destination number.

18 In the **IP Address** field, enter the IP address of the Signaling Server you use for system configuration and management.
If you selected a Signaling Server in step 1, enter the IP address of that Signaling Server.

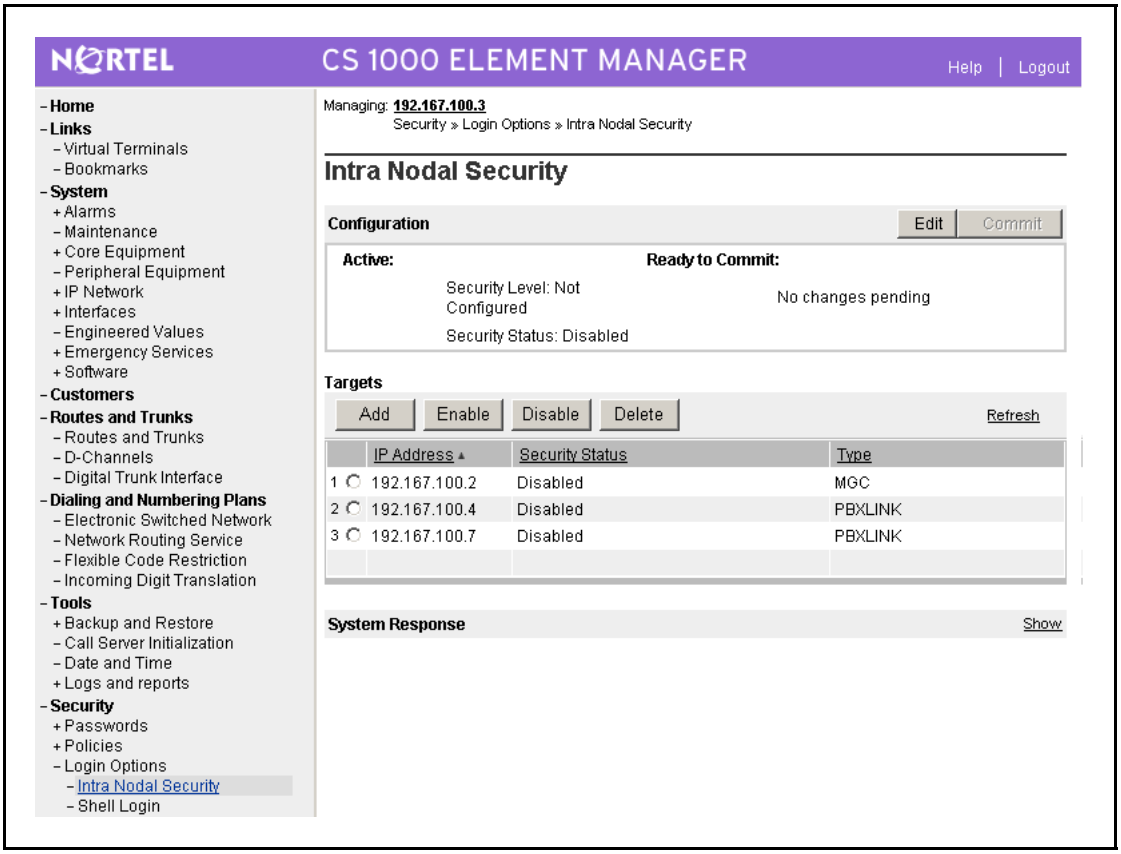
19 Click **Save**.

20 Log on to the call server using a PWD2 account.

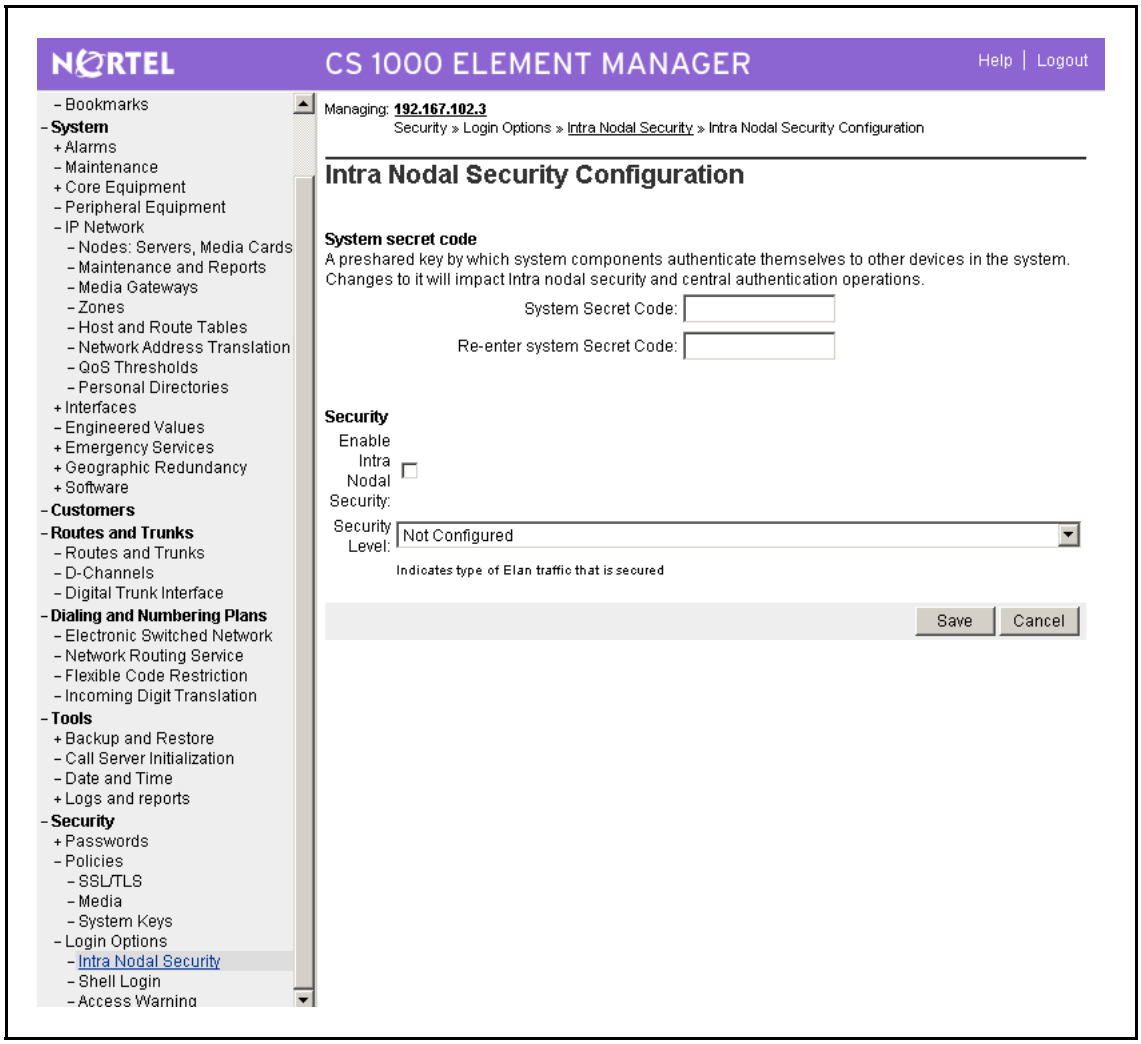
21 At the LD 43 prompt, enter
EDD
An Equipment Data Dump (EDD) occurs, and host route entries for new trap destinations are added to the network routing table for the Signaling Server, Voice Gateway Media Cards, and MGCs.

22 Log on to Element Manager on the local Signaling Server using a System password level 2 account.

23 Click **Security** > **Login Options** > **Intra Nodal Security**.
The **Intra Nodal Security** page appears.



24 In the Configuration pane, click **Edit**.
The **Intra Nodal Security Configuration** page appears.



25 In the **System Secret Code** field, enter the IPsec PSK.
Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key.

Record the PSK and store it in a safe place. You must enter the same value to configure ECM and to add or replace system elements.

26 In the **Re-enter System Secret Code** field, reenter the IPsec PSK.

27 Select the **Enable Intra Nodal Security** check box.

28 From the **Security Level** list, select a security level, which must be one of Optimized, Functional, or Full.

29 Click **Save**.
The **Intra Nodal Security** page appears, and the strength of the IPsec PSK appears in the **System Response** field.
Nortel recommends that you use a STRONG key; if the key

you entered is not STRONG, you can return to the **Intra Nodal Security Configuration** and enter a new key.

30 Click **Commit**.
A confirmation requestor appears.

31 Click **OK**.
A confirmation requestor appears.

32 Click **OK**.

33 Ensure that all system elements are reregistered and that ISSS is enabled.

--End--

Table 18
Variable Definitions

Variable	Value
<local Element Manager ELAN IP>	The IP address of the Signaling Server you selected in Step 1 of Procedure 1 “Configuring ISSS for the first time” (page 50).
<MGC ELAN IP Address>	The IP address of the MGC to add as an IPsec target.
<SignalingServer/VGMC IP Address>	The IP address of the Signaling Server or Voice Gateway Media Card to add as an IPsec target.

For more information about ISSS/IPsec security levels, see Table 17 "Job aid: ISSS/IPsec security levels" (page 48).

Table 19
Job aid: ISSS/IPsec security levels

ISSS/IPsec security level	Description
Optimized Security	(OPTI) Traffic over pbxLink and Xmsg between this host and its IPsec targets[1] is protected by IPsec. Any other traffic (other than pbxLink or Xmsg) between this host and its IPsec targets is permitted, but is NOT protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.
Functional Security	(FUNC) All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.

Table 19
Job aid: ISSS/IPsec security levels (cont'd.)

Full Security	(FULL)[3] All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is NOT permitted, except BootP, SSH (port 22), SSL (port 443), NTP (port 123), and AML (port 888). To connect with Element Manager on a signaling server over the ELAN when ISSS security policy Full is used, you must use HTTPS (HTTPS uses SSL).
Note[1] IPsec targets are either internal IPsec targets are that are added automatically when certain devices read IP addresses from a system configuration file and create IPsec targets for them, or external IPsec targets that are added from the command line. Note[2] ISSS neither blocks nor encrypts connections through the TLAN subnet. For VxWorks based hosts (Signaling Server, MGC, Voice Gateway Media Card), all traffic over the TLAN subnet is accepted over IP and is not encrypted. Note[3] ISSS security policy FULL is not available on the ECM host. If you configure the CS 1000 System to use ISSS security policy Full, configure the ECM to use ISSS security policy FUNC.	

Nortel recommends that you use a consistent naming convention when you add systems and devices as network elements. For an example of a typical naming convention, see Table 20 "Recommended naming for ECM network elements" (page 56).

Table 20
Recommended naming for ECM network elements

Element	Recommended naming convention	Example
CS 1000 system	<system name>	MyCompany_CS_A
CS 1000 Signaling Server	<system name>_<IP Telephony Node ID number>_Leader | Follower_1 | Follower_2 | Follower_n	MyCompany_CS_A_456_MyLeaderSS

ATTENTION
Nortel recommends that you enable ISSS before you use remote centralized Element Manager or certificate manager. However, even if you do not enable ISSS, you can securely use Element Manager on ECM (connected directly to a call server ELAN) to manage a single local CS 1000 system.

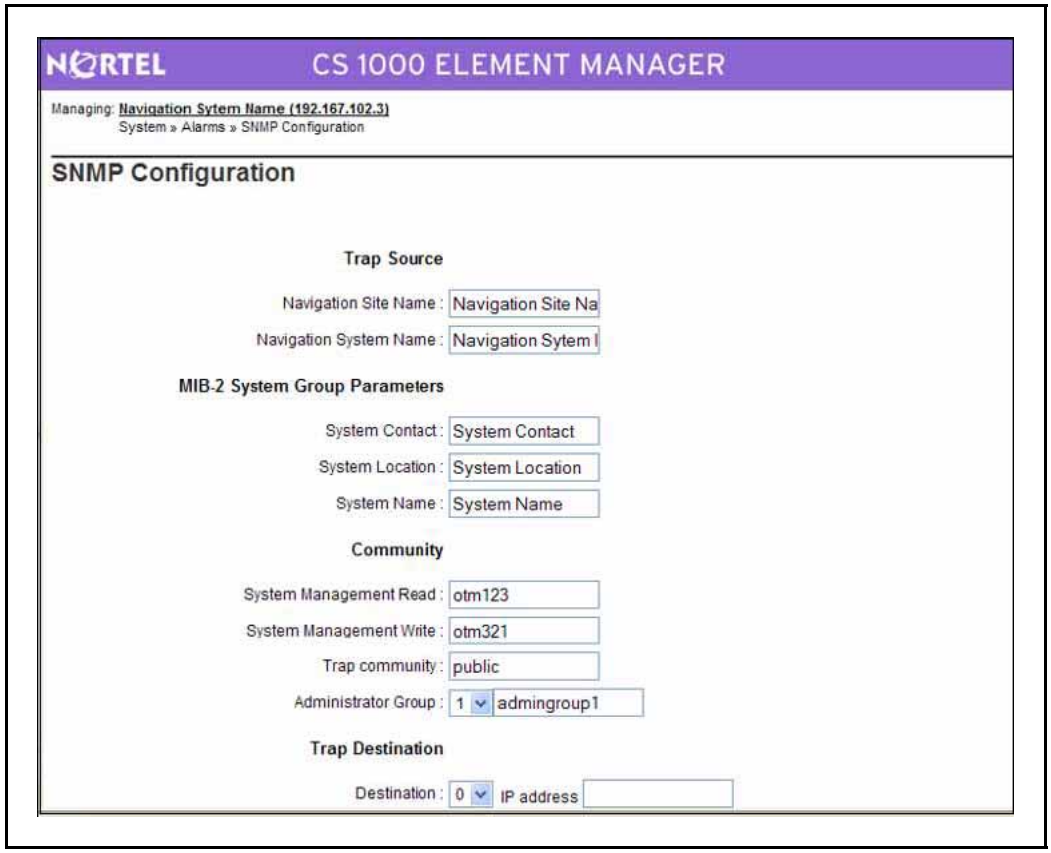
Use the following procedure to add a CS 1000 Release 5.0 or 5.5 system to the list of ECM managed elements, and configure IPsec on the system.

Part of this procedure involves creating SNMP trap destinations. This causes ELAN routes to be created from each device to Element Manager (these routes are needed for ISSS/IPsec to function), and also sends SNMP traps to Element Manager (for future development).

- Use the steps in Procedure 1 “Configuring ISSS for the first time” (page 50) to configure and enable ISSS/IPsec on the system.

Procedure 2
Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements

Step	Action
1	Log on to Element Manager on the local Signaling Server using a System password level 2 account.
2	Click **System** > **Alarms** > **SNMP**. The **SNMP Configuration** page appears.



3	In the **Destination** field, select a trap destination number.
4	In the **IP Address** field, enter the ELAN IP address of the remote centralized Element Manager on ECM.

5 Click **Save**.

6 Click **System** > **Alarms** > **SNMP**.
The **SNMP Configuration** page reappears.

7 In the **Destination** field, select a trap destination number.

8 In the **IP Address** field, enter the TLAN IP address of the remote centralized Element Manager on ECM.

9 Click **Save**.

10 Log on to the call server using a PWD2 account.

11 At the LD 43 prompt, enter
EDD
An Equipment Data Dump (EDD) occurs, and host route entries for new trap destinations are added to the network routing table for the Signaling Server, Voice Gateway Media Cards, and MGCs.

12 Using the local serial port or SSH, log on to the OAM shell.

13 Create an IPsec target for the ELAN interface on remote centralized Element Manager on ECM by entering:
isecNewTarget <remote ELEMENT MANAGER ELAN IP>

14 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

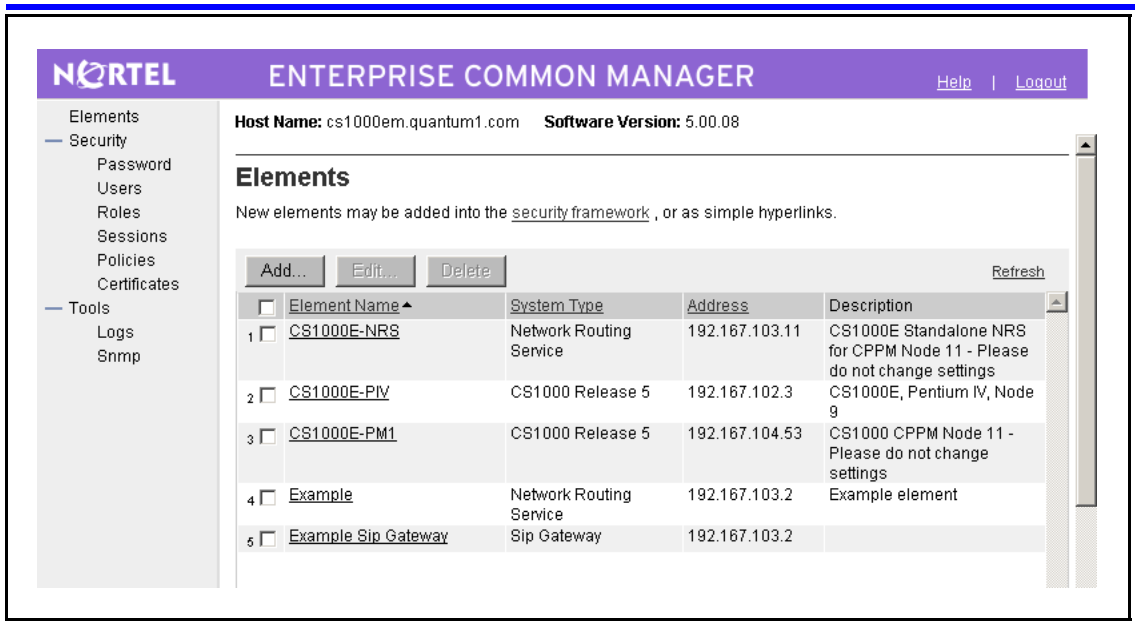
15 Create an IPsec target for the TLAN interface on remote centralized Element Manager on ECM by entering:
isecNewTarget <remote ELEMENT MANAGER TLAN IP>

16 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

17 Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.

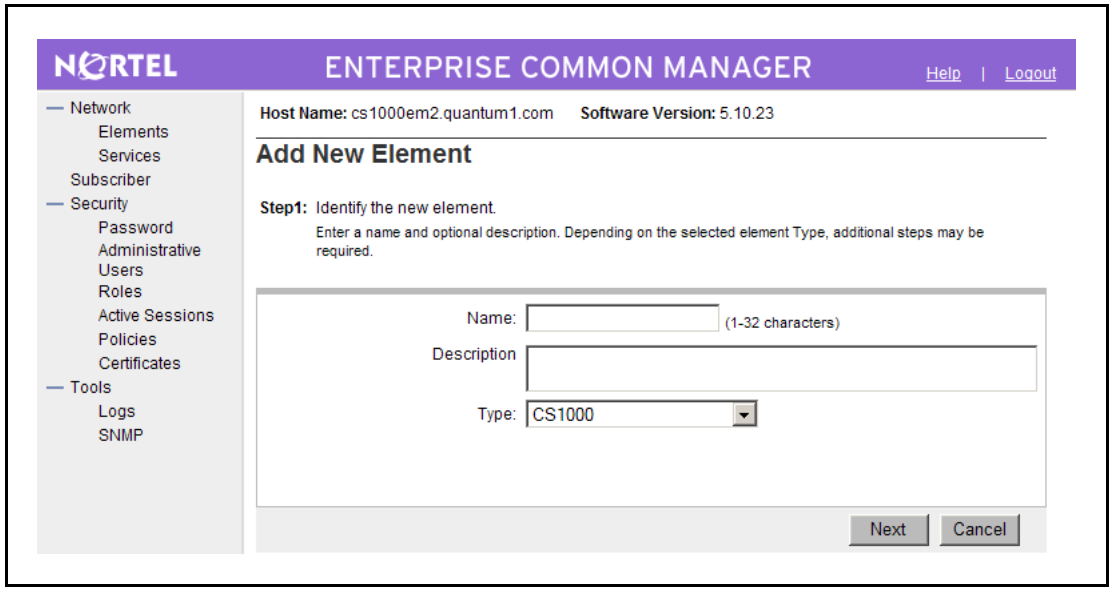
18 Click **Elements**.

The **Elements** page appears.



19 Click **Add**.

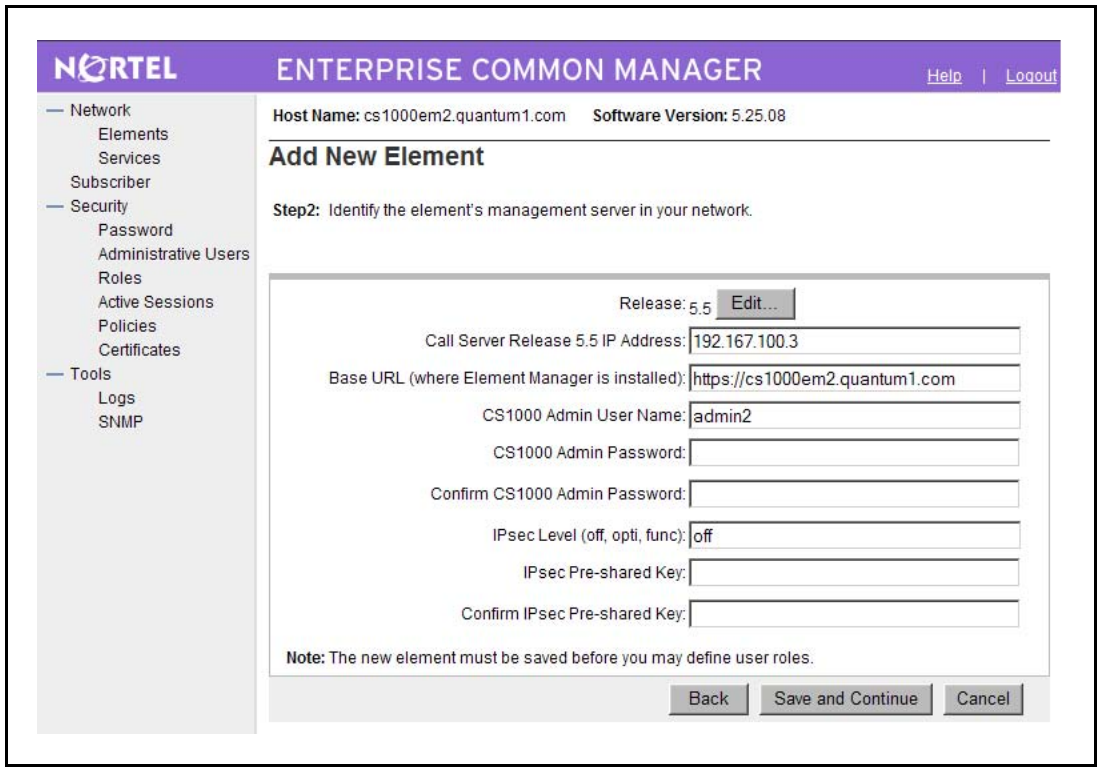
The **Add New Element Step1** page appears.



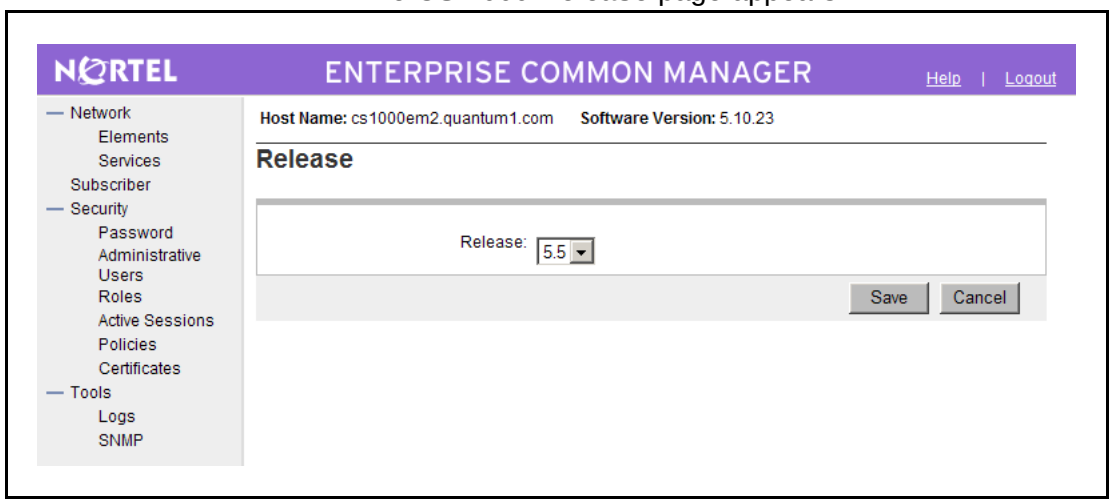
20 Perform the following actions:

- In the **Name** field, type an element name.
- In the **Description** field, type a description.
- From the **Type** list, select **CS1000**.

21 Click **Next**. The **Add New Element Step2** page appears.



22 Next to the **Release** field, click **Edit**.
The **CS 1000 Release** page appears.



23 From the **Release** menu, select the Call Server release (Release 5 or Release 5.5).
If you choose Release 5.5, the management URL is appended with the release number (for instance, emweb-5.5).

24 Click **Save** to return to the **Add New Element Step2** page.

25 In the **Call Server IP Address** field, type the ELNK Active IP address.

26 Enter the URL of the Element Manager on the ECM primary security server in the **Base URL** field

ATTENTION
Nortel recommends that you configure the Base URL to the URL of the Element Manager on the ECM primary security server. For any system where the Base URL points to another ECM, you must manually add IPsec targets on the ECM pointing to each signaling server.

27 In the **CS1000 Admin User Name** field, type a user name. The user name must match an existing user name on the CS 1000 system.

ATTENTION
The privilege level of the CS 1000 user name must match the privilege level of the user role that you use when you operate ECM. Therefore:

- If the ECM user has the Power User role, enter information for a CS 1000 admin2 account.
- If the ECM user has any other role, enter information for a CS 1000 admin1, admin2, or LAPW account.

28 In the **CS1000 Admin Password** field, type the password associated with the user name you entered in step 26.

29 In the **Confirm CS1000 Admin Password** field, retype the password.

30 In the **IPsec Level (off, opti, func)** field, type one of:

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

ATTENTION
Ensure that the ECM IPsec level and preshared key (PSK) are the same as the CS 1000 IPsec level and PSK; otherwise, communication between ECM and the system can be blocked. However, the ISSS security level Full is not available on ECM, so when the CS 1000 ISSS security level is Full, configure ECM ISSS security level to Func.

31 In the **IPsec Pre-shared Key** field, type the IPsec PSK.

32 In the **Confirm IPsec Pre-shared Key** field, type the IPsec PSK.

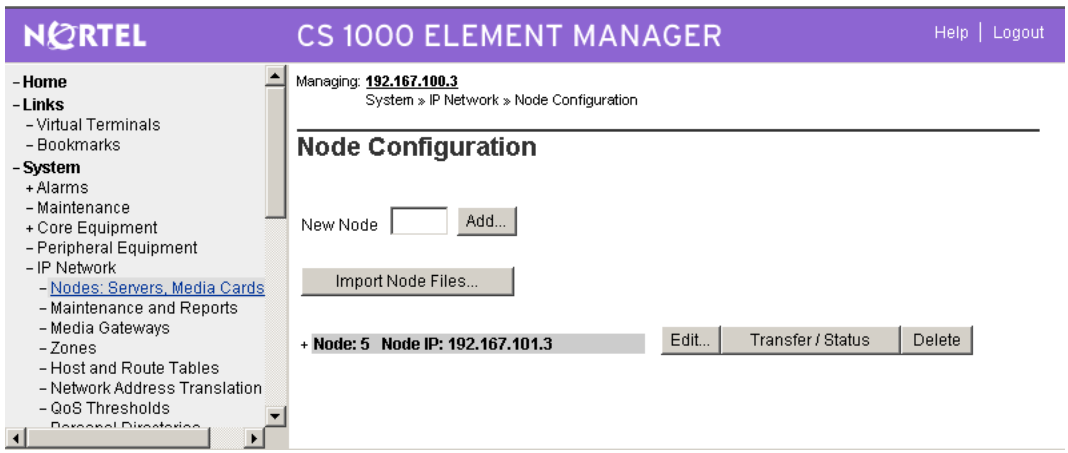
33 Click **Save and Continue**.

34 Log on to Element Manager on ECM.

35 Click **Elements**.
The **Elements** page appears.

36 Click on the Element Name that represents a CS 1000 Release 5.0 or 5.5 element.

37 Click **System** > **IP Network** > **Nodes: Servers, Media Cards**.
The **Node Configuration** page appears.



38 Click one of the node names listed.
Information about the node's element appears.

39 Log out of Element Manager.

40 Log in to Element Manager.

41 Click **System** > **IP Network** > **Nodes: Servers, Media Cards**.
The **Node Configuration** page reappears.

ATTENTION
The first time you click on an element, communication with the element fails, but this completes the ISSS initialization. The second time you click on the node, IPsec-secured communication is established.

42 Repeat steps 34 - 39 for or each CS 1000 Release 5.0 or 5.5 system you added to the list of ECM managed elements.

43 For each signaling server associated with the call servers you specified in this procedure, add it to the list of ECM managed elements by using the steps in Procedure 3 "Adding a Signaling Server to the ECM managed elements list to facilitate certificate management on the Signaling Server" (page 63).

--End--

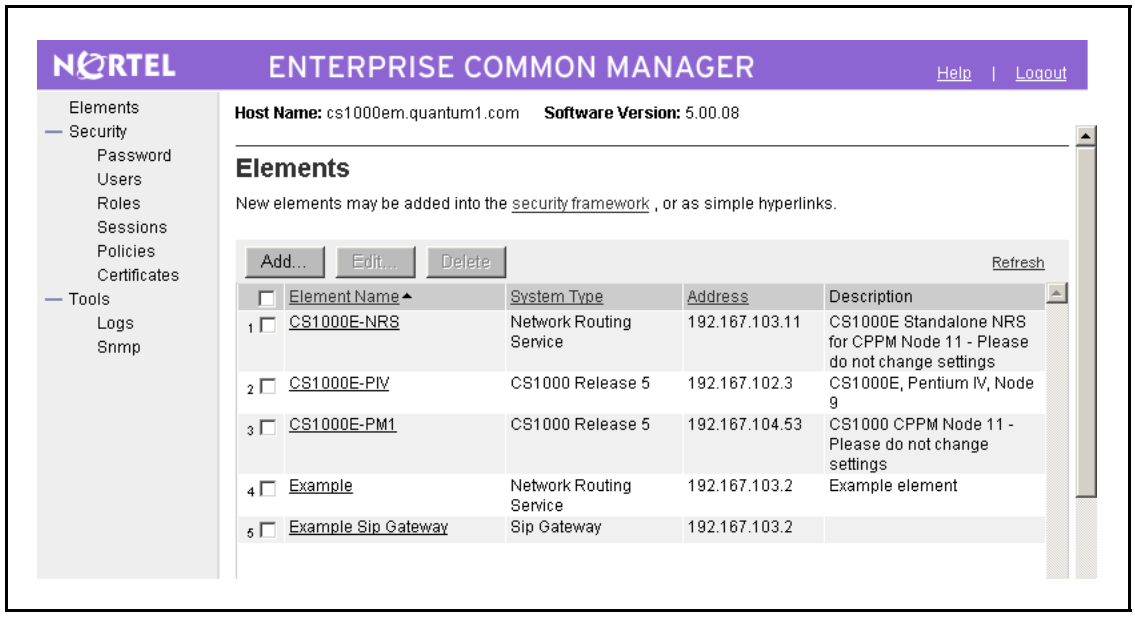
Table 21
Variable definitions

Variable	Value
<remote ELEMENT MANAGER ELAN IP>	The ELAN IP address of remote centralized Element Manager.
<remote ELEMENT MANAGER TLAN IP>	The TLAN IP address of remote centralized Element Manager.

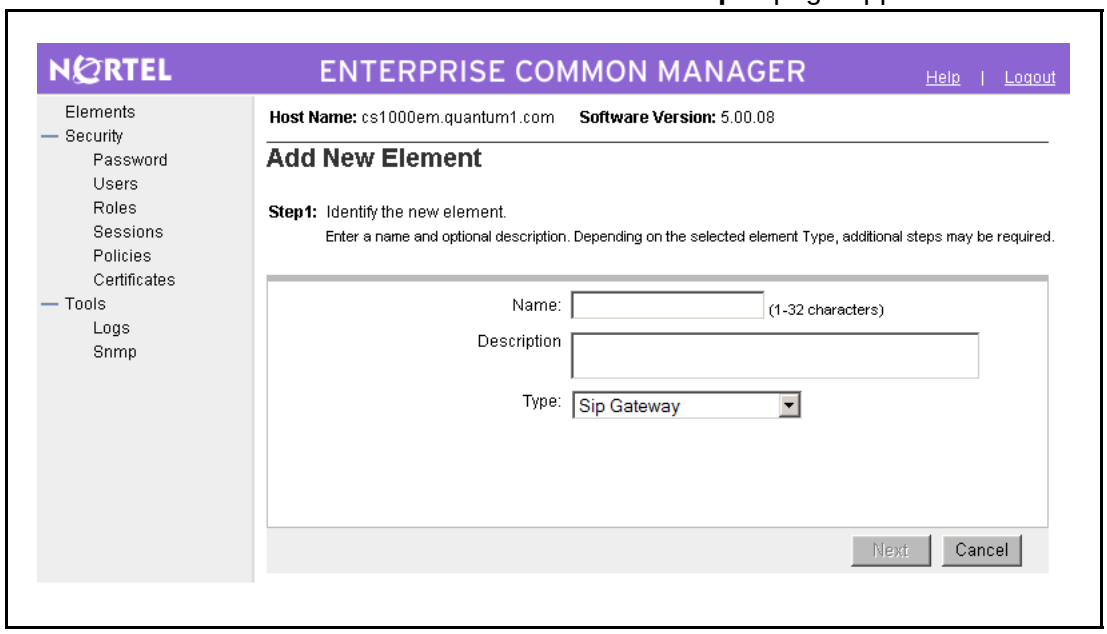
- Use local VxWorks-based Element Manager to configure and enable ISSS/IPsec on the system and add external IPsec targets pointing to the ELAN IP address of the Linux-based COTS server for the Element Manager on ECM. If you are using remote Element Manager on ECM, you must also add external IPsec targets pointing to the TLAN IP address.
- In the following procedure, if you choose not to use Element Manager on the ECM primary security server, you must then add the signaling servers as elements, and configure IPsec targets for the signaling servers from the ECM shell.

Procedure 3
Adding a Signaling Server to the ECM managed elements list to facilitate certificate management on the Signaling Server

Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Elements**. The **Elements** page appears.



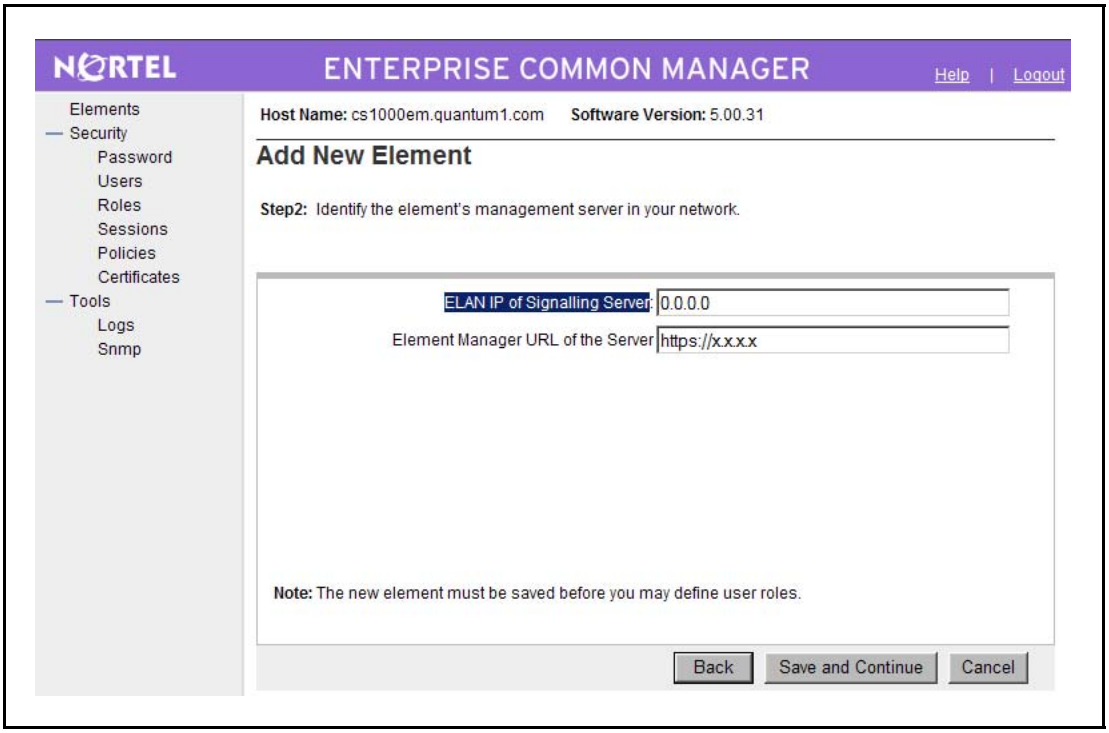
3 Click **Add**.
The **Add New Element Step1:** page appears.



4 Perform the following actions:

- In the **Name** field, type an element name.
  The name must be from 1 to 32 characters. Nortel recommends that you enter the host name.
- In the **Description** field, type a description.
- From the **Type** list, select **Sip Gateway**.

5 Click **Next**.
The **Add New Element Step2:** page appears.



6 Perform the following actions:

- In the **ELAN IP of Signalling Server** field, type the ELAN IP address for the Linux server.
- In the **Element Manager URL of the Server** field, type the NRS Manager URL.

7 Click **Save and Continue**.
The **Add New Element Step3:** page appears.

8 Click **Finish**.
For signaling servers that are members of CS 1000 Release 5.0 or 5.5 systems whose Element Manager URL points to the primary security server, you can now manage certificates.
For signaling servers that are members of CS 1000 Release 5.0 or 5.5 systems whose Element Manager URL points to an ECM server that is not the primary security server, or if the primary security server is coresident with NRS, then you must add IPsec targets pointing to each SIP Gateway Signaling Server, using the following steps:

9 Log on to the CLI of the ECM Linux host using the log on name nortel.

10 Enter the new IPsec target command:
`newipsectarget <SIP GW IP address> <IPsec PSK> <ISSS level>`

ATTENTION
If the IPsec PSK you enter contains any of the following special characters: !$%^&()_- +={}|\:;"'<,>.?/, you must precede each special character with a backslash (\).

A prompt appears requesting that you enter the root password.

11 Enter the root password.

12 Repeat step 9,10 and 11 for each SIP Gateway Signaling Server.

--End--

Table 22
Variable definitions

Variable	Value
<ISSS level>	The ISSS security level, which must be one of: • OPTI (optimal level, Xmsg and pbxLink messaging are secured) • FUNC (functional level, all packets traversing between Linux and any Node elements, including Call Server, are secured)
<IPsec PSK>	The PSK, which must be the same as the PSK used on the IPsec target.
<SIP GW IP address>	The IP address of the SIP Gateway Signaling Server to be configured as an IPsec target.

Prerequisites Use the following procedure to configure IPsec targets between two or more Linux hosts so that they can communicate using ISSS encryptions.

Procedure 4
Configuring ISSS between two Linux hosts

Step	Action
1	Log on to the CLI of the first ECM Linux host using the log on name nortel.
2	Enter the new IPsec target command: **`newipsectarget <IP address of Linux host 2> <IPsec PSK> <ISSS level>`** A prompt appears requesting that you enter the root password.
3	Enter the root password.
4	Log on to the CLI of the second ECM Linux host using the log on name nortel.

5 Enter the new IPsec target command:
newipsectarget <IP address of Linux host 1> <IPsec PSK> <ISSS level>
A prompt appears requesting that you enter the root password.

ATTENTION
If the IPsec PSK you enter contains any of the following special characters: !$%^&()_- +={}|\:;"'<,>.?/, you must precede each special character with a backslash (\).

6 Enter the root password.

7 Repeat steps 1-6 to establish targets between each Linux host and each other Linux host you have.

--End--

Table 23
Variable definitions

Variable	Value
<IP address of Linux host 1>	The IP address of the first Linux host.
<IP address of Linux host 2>	The IP address of the second Linux host.
<ISSS level>	The ISSS security level, which must be one of: • OPTI (optimal level, Xmsg and pbxLink messaging are secured) • FUNC (functional level, all packets traversing between Linux and any Node elements, including Call Server, are secured)
<IPsec PSK>	The PSK, which must be the same as the PSK used on the IPsec target.

ECM provides a group of shell scripts that you can use to configure and enable IPsec on Linux. The commands are stored in the directory /opt/nortel/ipsec and are listed in Table 24 "Job Aid: Linux shell scripts you can use to configure IPsec on Linux" (page 67).

Table 24
Job Aid: Linux shell scripts you can use to configure IPsec on Linux

Command	Description
newipsectarget <IP_address> <pre_shared_key> <ISSS_security_level>	This command creates a new IPsec target using the IP address, PSK, and ISSS security level you enter as arguments. It also sends a packet to the IPsec target to trigger the negotiation of IPsec security associations.

Table 24
Job Aid: Linux shell scripts you can use to configure IPsec on Linux (cont'd.)

Command	Description
deleteipsectarget <IP_address>	This command deletes an existing IPsec target for the IP address you enter as an argument.
printipsecpolicy	This command prints security policies configured for each IPsec target, including the ISSS security level (OFF, OPTI, or FUNC), IPsec protocol being used (currently only ESP is used), and IPsec mode being used (currently only Transport mode is used).
checkIPsecStatus	This command checks the status of each IPsec target, including current IPsec configuration (enabled or disabled) for this target, the TCP connectivity to the Xmsg server on this target when IPsec is disabled, and the TCP connectivity to the Xmsg server on this target when IPsec is enabled.

Add, remove, or replace a CS 1000 system element when ISSS is enabled and active

Use the procedures in this section to add, remove, repair, or replace a CS 1000 system element when ISSS is enabled.

If you are installing a component that was previously installed and configured to use ISSS, log on to the local CLI of the component, and decommission IPsec. For more information about decommissioning IPsec on a component, see Procedure 112 "Decommissioning IPsec locally by using CLI" (page 285).

Recommended methods to add, remove, or replace a system element

ATTENTION
Nortel recommends that you use Element Manager on the local Signaling Server to complete the following procedure. It is also possible to complete this procedure using local Element Manager on ECM, or using the remote centralized Element Manager on ECM; however, using either of those methods requires additional steps, and is not recommended.

Use the procedures in this section to:

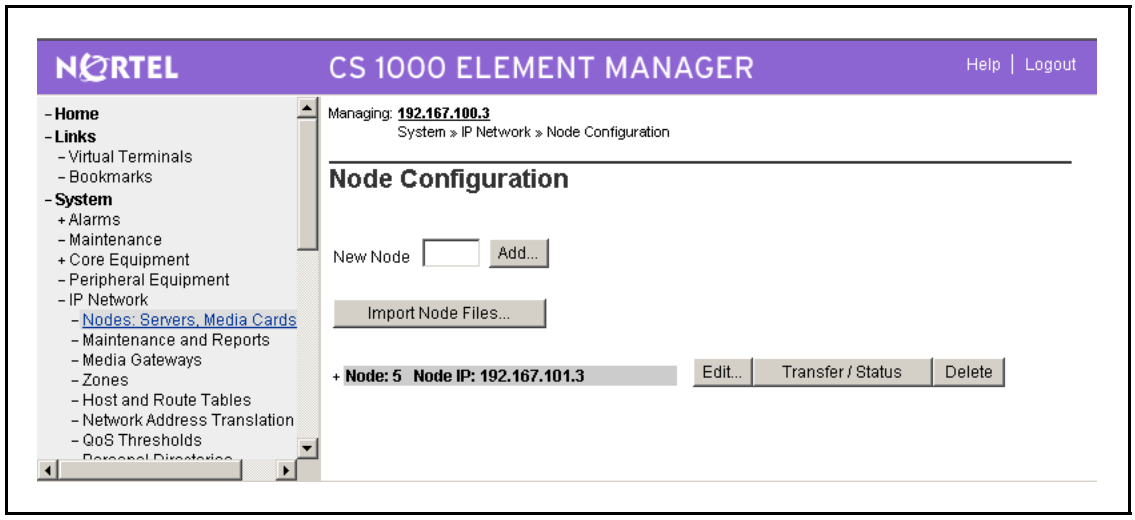
- Add a new leader or follower Signaling Server, MGC, MC32S, or Voice Gateway Media Card
- Replace the hardware and reconfigure the ELAN interface MAC address of an existing follower system element whose hardware must be replaced. Complete this task in the following situations:
  - When Signaling Server or Voice Gateway Media Card hardware failure occurs.
  - When changing the SRTP (upgrade to MC32S required) or RFC2833 (upgrade to MC32 or MC32S required) capability (Voice Gateway Media Card).
  - When changing the Signaling Server host server capacity by replacing ISP1100 with VxWorks-based Commercial Off The Shelf (COTS), or CP PM Signaling Server.

Use the following procedure to add a follower Voice Gateway Media Card or follower Signaling Server when ISSS is enabled.

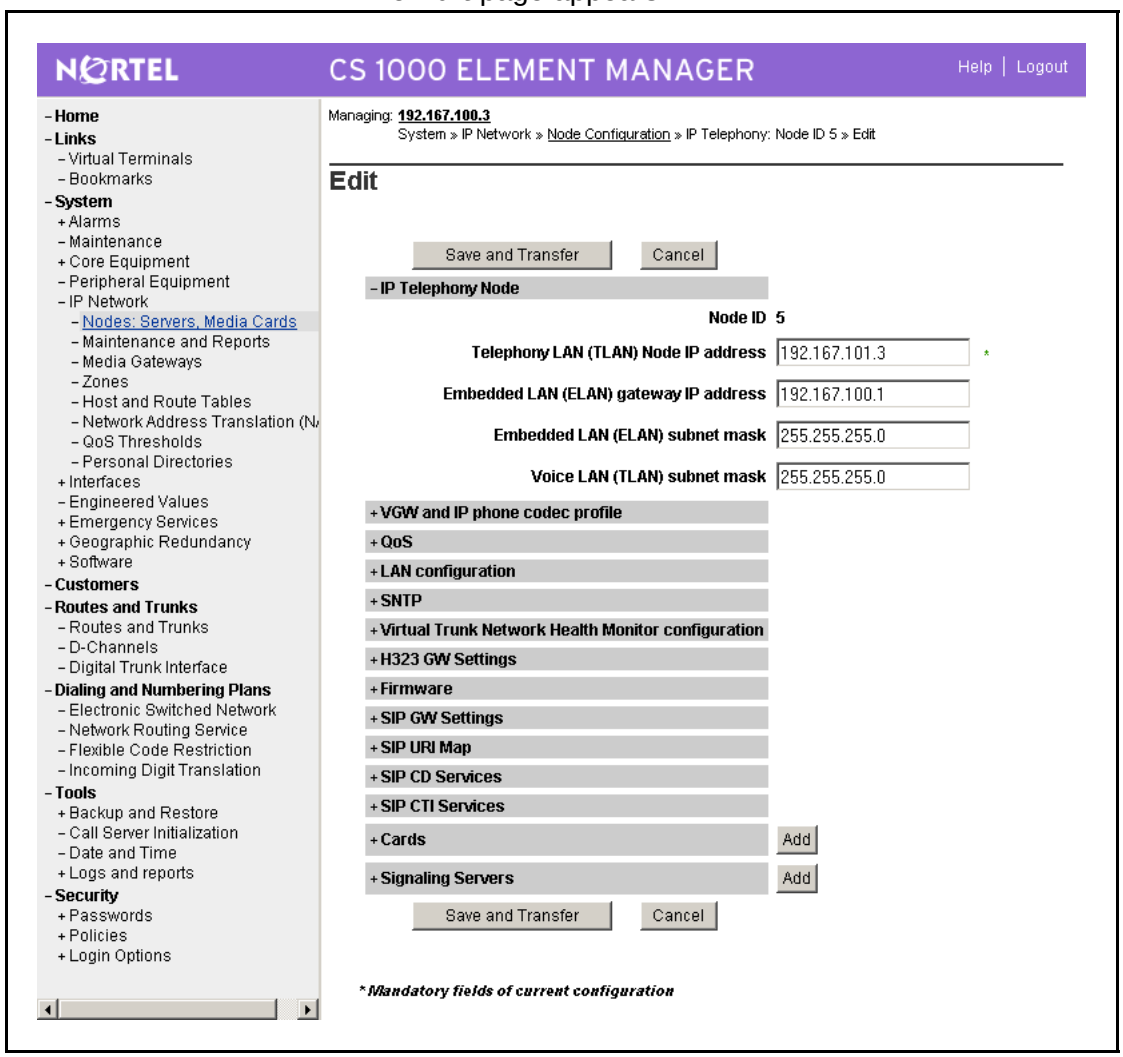
Procedure 5
Adding or replacing a follower Voice Gateway Media Card or follower Signaling Server when ISSS is enabled

ATTENTION
This procedure does not apply to MC32S. To add or replace an MC32S, see Procedure 8 “Adding or replacing an MC32S when ISSS is enabled” (page 85).

Step	Action
1	Log on to Element Manager on the local Signaling Server that you selected and configured in Procedure 1 “Configuring ISSS for the first time” (page 50), **OR** Log on to the remote centralized Element Manager on ECM.
2	Click **System** > **IP Network** > **Nodes: Servers, Media Cards**. The Node Configuration page appears.



3 Click **Edit** next to the node for which you want to add or replace an element.
The **Edit** page appears.



4 Complete one of the following:

If you are adding a new device (Voice Gateway Media Card or Signaling Server):

- click **Add** next to the type of device you are adding
- enter IP Telephony Node configuration settings for the device you are adding.

OR

If you are replacing an existing device (Voice Gateway Media Card or Signaling Server):

- expand the section for the type of device you are replacing
- expand the entry for the device you are replacing
- enter the MAC address for the new device.

5 Click **Save and Transfer**.
An error message appears that indicates changes were not transferred to the new device.

6 Restart the new device.
During restart, the new follower device receives BOOTP information, including its ELAN IP address, from the leader.

7 Using the local serial port or SSH, log on to the shell of the new device (the IPL shell if you are adding or replacing a Voice Gateway Media Card, or the OAM shell if you are adding or replacing the Signaling Server).

8 Enter the IPsec new target command to create an IPsec target for the Call Server:
isecNewTarget <CALL SERVER ELNK ACTIVE IP>

9 Enter the enable IPsec target command:
isecEnlTarget <CALL SERVER ELNK ACTIVE IP>

10 Enter the IPsec new target command to create an IPsec target for local Element Manager :
isecNewTarget <local ELEMENT MANAGER ELAN IP>

11 Enter the enable IPsec target command:
isecEnlTarget <local ELEMENT MANAGER ELAN IP>
If you do not have remote centralized Element Manager on ECM, proceed to step 16.

12 Enter the IPsec new target command to create an IPsec target for the ELAN interface of the remote centralized Element Manager on ECM:
isecNewTarget <remote ELEMENT MANAGER ELAN IP>

13 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

14 Enter the IPsec new target command to create an IPsec target for the TLAN interface of the remote centralized Element Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER TLAN IP>

15 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

16 Enter the change IPsec PSK command:
isecChgPSK
The following prompt appears:

```
Are you sure you want to continue?  (Yes/[No]):
```

17 Enter **yes** to confirm that you want to change the IPsec PSK.

18 Enter the new IPsec PSK.

Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key.

A prompt appears that requests confirmation of the new IPsec PSK.

19 Reenter the new PSK.

The device saves the IPsec PSK.

20 Enter the IPsec Change level command
isecChgLevel "[OPTI/FUNC/FULL]"

The following prompt appears: `Are you sure you want to continue?  (Yes/[No]):`

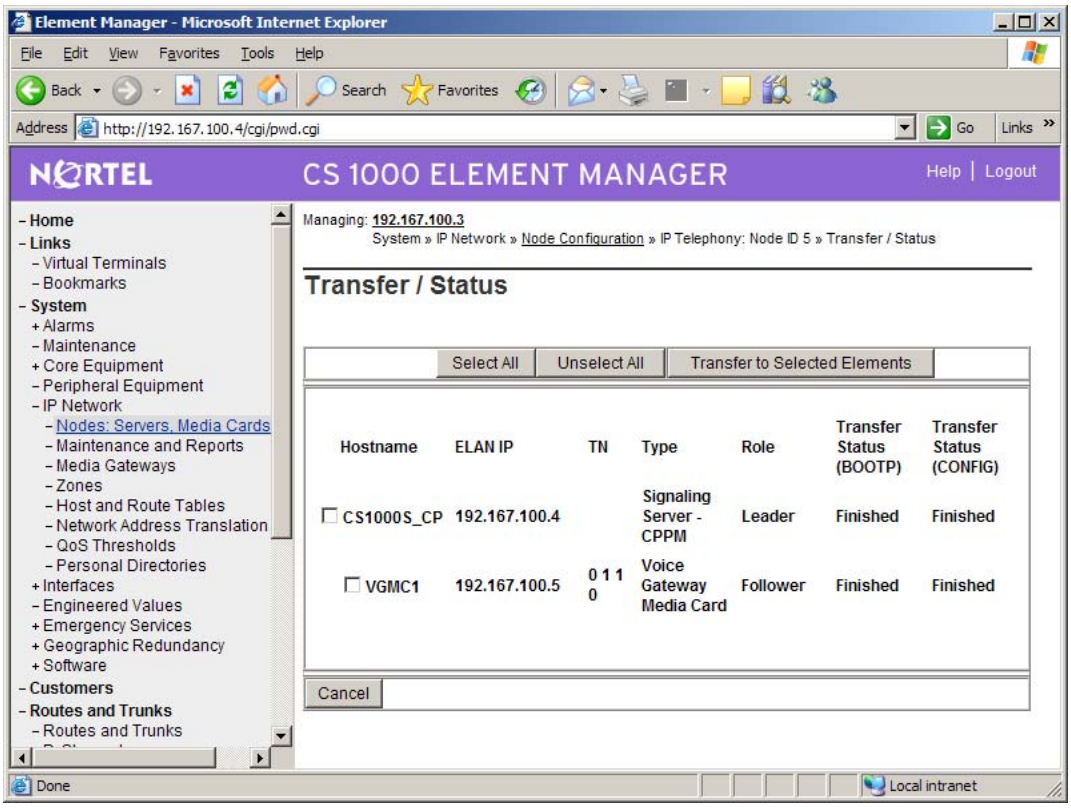
21 Enter:
yes
The ISSS security level is configured, and ISSS is enabled.

22 Enter the following command to ensure that the pbxLink with the new device is active:
pbxLinkShow
The pbxLink status appears.

23 Log on to Element Manager on the local Signaling Server that you targeted in step 10.

24 Click **System** > **IP Network** > **Nodes: Servers, Media Cards**.
The **Node Configuration** page appears.

25 Click **Transfer/Status** next to the node of which the new device is a part.
The **Transfer/Status** page appears.



26 Verify that the Transfer status columns contain a value of *Finished*.

27 Click **Security** > **Login Options** > **Intra Nodal Security** to return to the **Intra Nodal Security** page.

28 Click **Edit**.
The **Intra Nodal Security Configuration** page appears.

29 Perform the following steps to disable and then reenable ISSS to send the current ISSS system status to the new device:
Clear the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.

Click **Edit** to return to the **Intra Nodal Security** page.
Check the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.
Click **Commit** to transmit the ISSS target information.

--End--

Table 25
Variable definitions

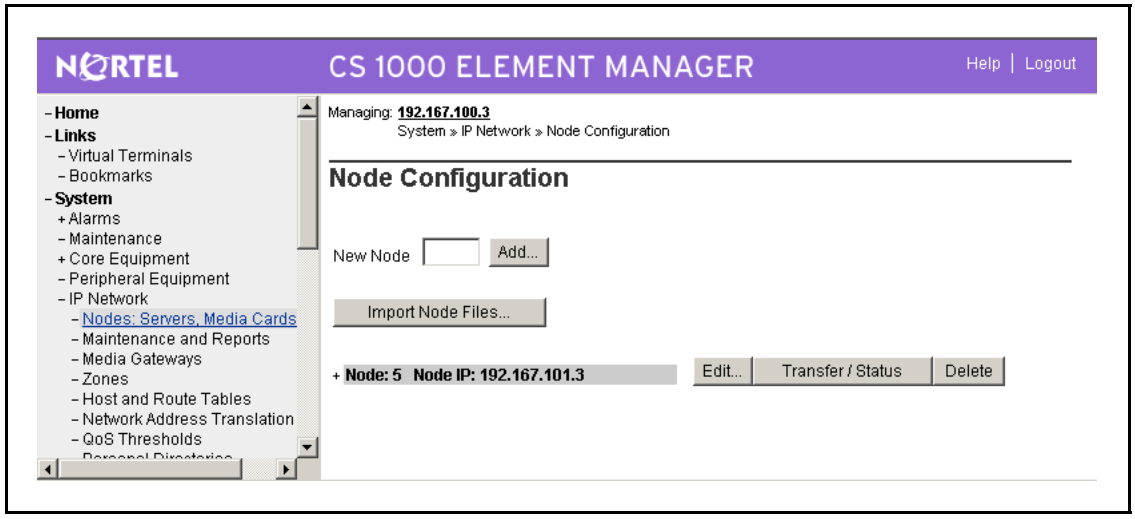
Variable	Value
<CALL SERVER ELNK ACTIVE IP>	The ELNK ACTIVE IP address of the call server.
<ACTIVE CP IP ADDRESS>	The address of the Call Server Active CP.
<ELEMENT MANAGER IP ADDRESS>	The address of Element Manager on the local Signaling Server.
<local ELEMENT MANAGER ELAN IP>	The ELAN IP address of a local Element Manager Signalling Server host that is in the same IP telephony node as the new device[1].
<remote ELEMENT MANAGER ELAN IP>	The ELAN IP address of remote centralized Element Manager.
<remote ELEMENT MANAGER ELAN IP>	The TLAN IP address of remote centralized Element Manager.
Note[1]: If you add a Voice Gateway Media Card to a node that contains only Voice Gateway Media Cards, Nortel recommends that you use the same Signaling Server host for all the Voice Gateway Media Cards in the node.	

Use the following procedure to add a leader Voice Gateway Media Card when ISSS is enabled.

ATTENTION
When ISSS is enabled, you must add or replace new devices using Element Manager on a Signaling Server that is in the same IP Telephony node where you are adding or replacing the device.

Procedure 6
Adding or replacing a leader Voice Gateway Media Card when ISSS is enabled

Step	Action
1	Log on to Element Manager on the local Signaling Server that you selected and configured in Procedure 1 “Configuring ISSS for the first time” (page 50), **OR** Log on to the remote centralized Element Manager on ECM.
2	Click **System** > **IP Network** > **Nodes: Servers, Media Cards**. The Node Configuration page appears.

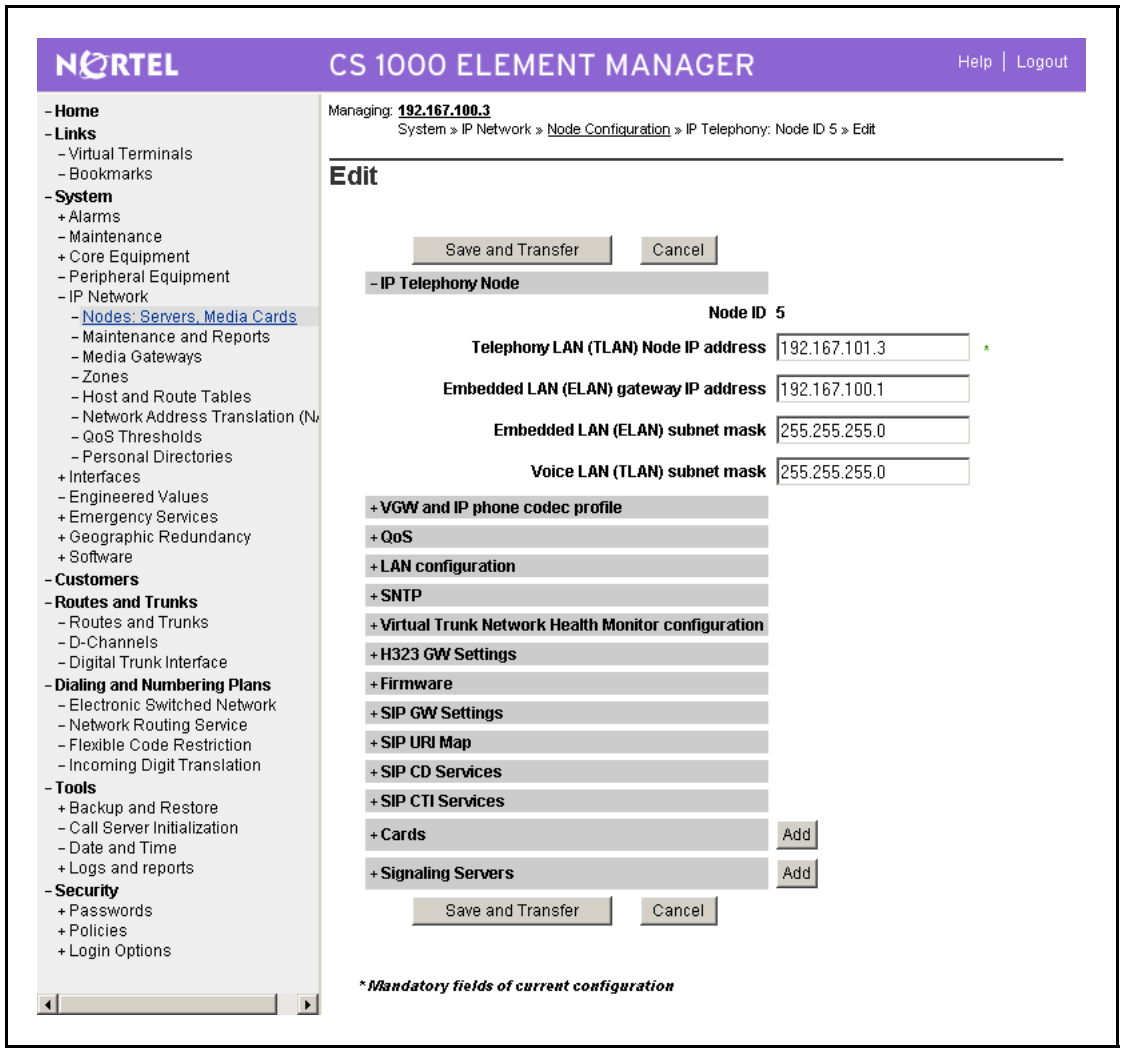


If you are replacing a Voice Gateway Media Card, proceed to step 5.

3 If you are adding a new leader Voice Gateway Media Card, you must add a new node for which it is to be the leader. Enter the new node number in the **New Node** field.

4 Click **Add** to create the new node.

The **Edit** page appears.



Proceed to step 6.

5 If you are replacing a Voice Gateway Media Card, click **Edit** next to the node for which you want to add or replace an element. The **Edit** page appears.

6 Complete one of the following:

If you are adding a new Voice Gateway Media Card:

- click **Add** next to **Cards**
- enter IP Telephony Node configuration settings for the device you are adding.

OR

If you are replacing an existing Voice Gateway Media Card:

- expand the Card section
- expand the entry for the device you are replacing
- enter the MAC address for the new device.

7 Click **Save and Transfer**.
An error message appears that indicates changes were not transferred to the new device.

8 Using the local serial port or SSH, log on to the IPL shell of the new Voice Gateway Media Card.

9 Enter the set leader command:
setLeader "<leader ELAN IP>","<SUBNET MASK>","<ELAN IP Gateway>".
The three parameters must each be enclosed in double quotation marks. There must be a space after the command and before the first parameter. Put commas and no spaces between the parameters.

10 Restart the Voice Gateway Media Card.

11 Using the local serial port or SSH, log on to the IPL shell of the new Voice Gateway Media Card.

SSH is not available for a short period of time after you restart the new device. If you are unable to connect using SSH, wait one minute, and try again.

12 Enter the IPsec new target command to create an IPsec target for the Call Server:
isecNewTarget <CALL SERVER ELNK ACTIVE IP>

13 Enter the enable IPsec target command:
isecEnlTarget <CALL SERVER ELNK ACTIVE IP>

14 Enter the IPsec new target command to create an IPsec target for local Element Manager :
isecNewTarget <local ELEMENT MANAGER ELAN IP>

15 Enter the enable IPsec target command:
isecEnlTarget <local ELEMENT MANAGER ELAN IP>
If you do not have remote centralized Element Manager on ECM, proceed to step 12.

16 Enter the IPsec new target command to create an IPsec target for the ELAN interface of the remote centralized Element Manager on ECM:
isecNewTarget <remote ELEMENT MANAGER ELAN IP>

17 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

18 Enter the IPsec new target command to create an IPsec target for the TLAN interface of the remote centralized Element

Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER TLAN IP>

19 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

20 Enter the IPsec change PSK command:
isecChgPSK.
The following prompt appears:

```
Are you sure you want to continue?  (Yes/[No]):
```

21 Confirm that you want to change the IPsec PSK by entering:
yes

22 Enter the new IPsec PSK.

Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key.

A prompt appears that requests confirmation of the new IPsec PSK.

23 Reenter the new PSK.

The device saves the IPsec PSK.

24 Enter the IPsec Change level command
isecChgLevel [OPTI/FUNC/FULL]

The following prompt appears: `Are you sure you want to continue?  (Yes/[No]):`

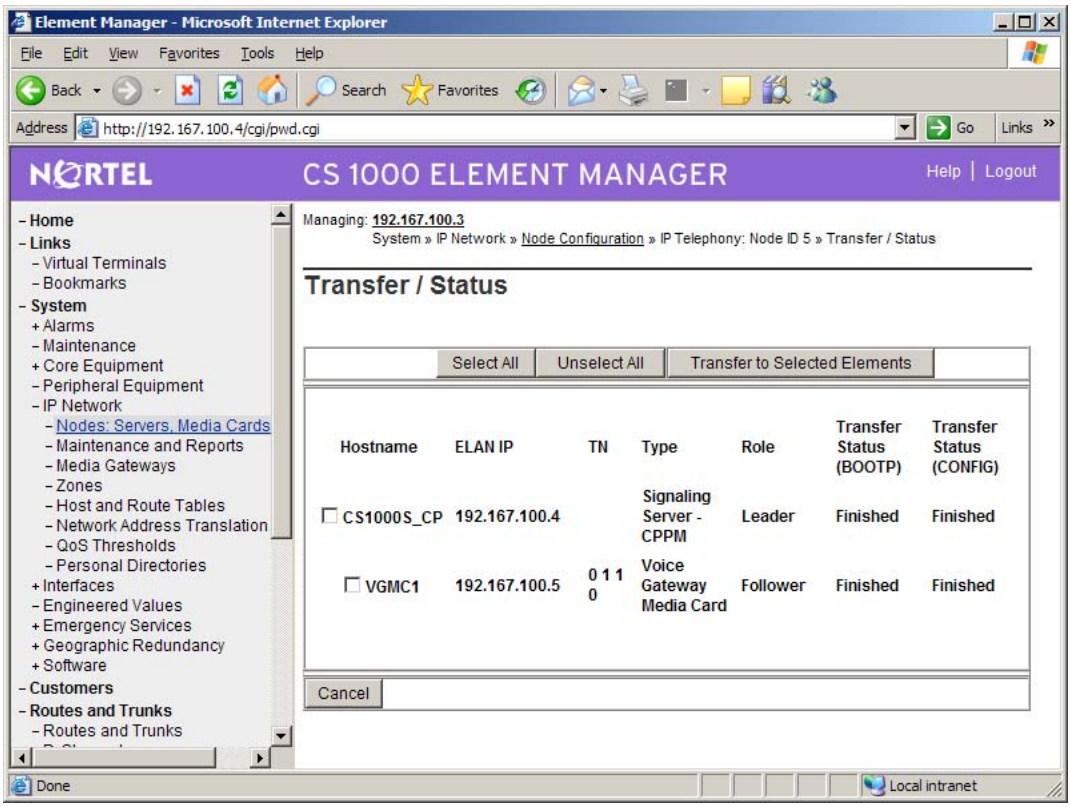
25 Enter:
yes
The ISSS security level is configured, and ISSS is enabled.

26 Enter the following command to ensure that the pbxLink with the new device is active:
pbxLinkShow
The pbxLink status appears.

27 Log on to Element Manager on the Signaling Server that you targeted in step 6 of this procedure.

28 Click **System** > **IP Network** > **Nodes: Servers, Media Cards** to return to the Node Configuration page.

29 Click **Transfer/Status** next to node of which the new device is a part.
The **Transfer/Status** page appears.



30 Verify that the Transfer status columns contain a value of *Finished*.

31 Click **Security** > **Login Options** > **Intra Nodal Security** to return to the **Intra Nodal Security** page.

32 Click **Edit**.
The **Intra Nodal Security Configuration** page appears.

33 Perform the following steps to send the current ISSS system status to the new device:
Clear the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.

Click **Edit** to return to the **Intra Nodal Security** page.
Check the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.
Click **Commit** to transmit the ISSS target information.

--End--

Table 26
Variable definitions

Variable	Value
<ACTIVE CP IP ADDRESS>	The address of the Call Server Active CP.
<CALL SERVER ELNK ACTIVE IP>	The ELNK ACTIVE IP address of the call server.
<ELAN IP Gateway>	The ELAN IP Gateway.
<ELEMENT MANAGER ELAN IP>	The ELAN IP address of an Element Manager Signalling Server host that is in the same IP telephony node as the new device.
<ELEMENT MANAGER IP ADDRESS>	The address of Element Manager on the local Signaling Server.
<leader ELAN IP>	The ELAN IP address of the new leader.
<SUBNET MASK>	The ELAN subnet mask of the new leader.

ATTENTION
When ISSS is enabled, add or replace new devices using the Element Manager that you selected and configured in "First-time configuration and activation of ISSS" (page 48), or using remote centralized Element Manager on ECM.

If you add a Signaling Server and your system includes remote Element Manager on ECM that you plan to use for Certificate Management of it, then you must complete the steps in Procedure 3 "Adding a Signaling Server to the ECM managed elements list to facilitate certificate management on the Signaling Server" (page 63).

Use the following procedure to add a leader Signaling Server when ISSS is enabled. For information about using the Signaling Server Installation Tool, see *Signaling Server Installation and Commissioning (NN43001-312)* () .

Procedure 7
Adding or replacing a leader Signaling Server when ISSS is enabled

Step	Action
1	Start the Signaling Server Software Installation Tool on the Signaling Server. The `Installation Tool Main Menu` appears.

2	Enter:
	e
	`To perform basic Signaling Server configuration only.`
	The following output appears:
	`Please insert the database diskette in the`

removable drive to restore the IP configuration to the hard disk.

3 Enter:
b
Continue without restoring the IP configuration.
The following output appears: Please select the role of this Signaling Server.

4 Enter:
a
Set this Signaling Server as a Leader.
The following output appears: Please select the application configuration for this Signaling Server.

5 Enter:
a
Co-resident (LTPS/VTRK/NRS).
The following output appears: Please select the Network Routing Service (NRS) configuration for this Signaling Server.

6 Enter:
a
H.323 Gatekeeper and SIP Redirect/Proxy Server.
The following output appears: Please select the type of Network Routing Service (NRS) for this Signaling Server.

7 Enter:
a
Primary.
The following output appears: Please enter the data networking and IP Telephony parameters for this Leader Signaling Server.

8 Enter the parameters, including the ELAN IP address, for the new leader Signaling Server.

9 Restart the new Signaling Server.
During restart, the new leader Signaling Server receives BOOTP information, including its own ELAN IP address, from the leader.

10 Using the local serial port or SSH, log on to the IPL shell of the new Voice Gateway Media Card.

11 Enter the IPsec new target command to create an IPsec target for the Call Server:
isecNewTarget <CALL SERVER ELNK ACTIVE IP>

12 Enter the enable IPsec target command:
isecEnlTarget <CALL SERVER ELNK ACTIVE IP>

13 Enter the IPsec new target command to create an IPsec target for local Element Manager :
isecNewTarget <local ELEMENT MANAGER ELAN IP>

14 Enter the enable IPsec target command:
isecEnlTarget <local ELEMENT MANAGER ELAN IP>
If you do not have remote centralized Element Manager on ECM, proceed to step 19.

15 Enter the IPsec new target command to create an IPsec target for the ELAN interface of the remote centralized Element Manager on ECM:
isecNewTarget <remote ELEMENT MANAGER ELAN IP>

16 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

17 Enter the IPsec new target command to create an IPsec target for the TLAN interface of the remote centralized Element Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER TLAN IP>

18 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

19 Enter the command **isecChgPSK** to change the IPsec PSK. The following prompt appears:

```
Are you sure you want to continue?  (Yes/[No]):
```

20 Enter **yes** to confirm that you want to change the IPsec PSK.

21 Enter the new IPsec PSK.

Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key.

A prompt appears that requests confirmation of the new IPsec PSK.

22 Reenter the new IPsec PSK.

The device saves the IPsec PSK.

23 Enter the IPsec Change level command
isecChgLevel [OPTI/FUNC/FULL]

The following prompt appears: `Are you sure you want to continue?  (Yes/[No]):`

24 Enter:
yes
The ISSS security level is configured, and ISSS is enabled.

25 Enter the following command to ensure that the pbxLink with the new device is active:

pbxLinkShow
The pbxLink status appears.

26 Log on to Element Manager on the Signaling Server that you targeted in step 13 of this procedure.

27 Click **System** > **IP Network** > **Nodes: Servers, Media Cards** to return to the Node Configuration page.

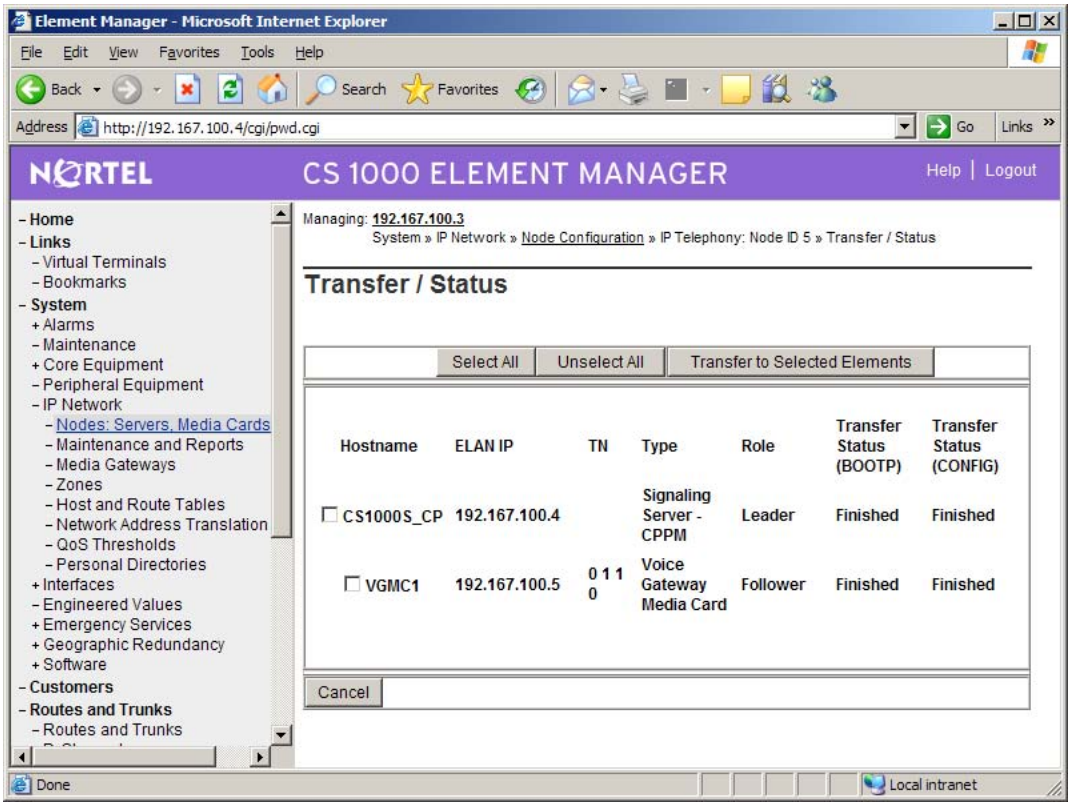
If you are adding a new Signaling Server, proceed to step 30.

28 If you are replacing a Signaling Server, click **Edit**.
The **Edit** page appears.

29 Complete the following:

- expand the section for the type of device you are replacing
- expand the entry for the device you are replacing
- enter the MAC address for the new device.

30 Click **Transfer/Status** next to the node of which the new device is a part.
The **Transfer/Status** page appears.



31 Verify that the Transfer status columns contain a value of *Finished*.

32 Click **Security** > **Login Options** > **Intra Nodal Security** to return to the **Intra Nodal Security** page.

33 Click **Edit**.
The **Intra Nodal Security Configuration** page appears.

34 Perform the following steps to send the current ISSS system status to the new device:
Clear the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.

Click **Edit** to return to the **Intra Nodal Security** page.
Check the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.
Click **Commit** to transmit the ISSS target information.

--End--

ATTENTION
If you replace the Signaling Server you selected in step 1 of Procedure 1 "Configuring ISSS for the first time" (page 50), then you must repeat steps 2 through 8 of that procedure to create targets on the new Signaling Server pointing to each MGC in the system, and to each Signaling Server and each Voice Gateway Media Card in each IP Telephony Node, except those in the same node as the selected Signaling Server.

Table 27
Variable definitions

Variable	Value
<ACTIVE CP IP ADDRESS>	The address of the Call Server Active CP.
<CALL SERVER ELNK ACTIVE IP>	The ELNK ACTIVE IP address of the call server.
<ELEMENT MANAGER ELAN IP>	The ELAN IP address of an Element Manager Signalling Server host that is in the same IP telephony node as the new device.
<ELEMENT MANAGER IP ADDRESS>	The address of Element Manager on the local Signaling Server.

Use the following procedure to add or replace a leader or follower MC32S when ISSS is enabled.

Procedure 8
Adding or replacing an MC32S when ISSS is enabled

Step	Action
1	Log on to the CLI on the MC32S you are adding. The following message appears: **This is the MC32S Gold Image. The vxWorks Image on /p/mainos.sys failed to load.** **The system has not been installed or there is a problem with the compact flash** **Please use setLeader command to enter networking parameters.** **Then Install system software using Element Manager or TM** If message shown above does not appear, then the card has been previously installed. If that is the case, enter the Leading Secondary Call Server IP address in step 10, instead of the Signaling Server IP address, and omit steps 27-38.

2	Enter:
	mc32ssetup
	The following prompt appears:
	`Please define the data networking parameters for this MC32S now.`
	`Hostname :`

3	Enter the host name. The following prompt appears: `ELAN IP :`
4	Enter the ELAN IP address of the new device. The following prompt appears: `ELAN subnet mask:`
5	Enter the ELAN subnet mask. The following prompt appears: `ELAN gateway:`
6	Enter the ELAN gateway IP address. The following prompt appears: `Primary CS Hostname:`
7	Enter the Host Name for the of the Primary Call Server. The following prompt appears: `Primary CS IP:`
8	Enter the IP address of the primary Call Server. The following prompt appears: `Leading Secondary CS Hostname:`

9 Enter the Host Name for the of the Leading Secondary Call Server.

The following prompt appears:
```
Leading Secondary CS IP:
```

10 Enter the IP address of the local signaling server that is running Element Manager.

> **ATTENTION**
> This step temporarily configures Leading Secondary Call Server value to use the IP address of the signaling server on which Element Manager is running. This allows the new MC32S card to download updated loadware from the signaling server.

The following prompt appears:
```
Secondary CS Hostname:
```

11 Enter the Host Name of the Secondary Call Server.

The following prompt appears:
```
Secondary CS IP:
```

12 Enter the IP address of the secondary Call Server.

The following prompt appears:
```
Do you want to configure this card as a leader?
(y/n/[a]bort) :
```

13 Enter:
```
y
```
The following prompt appears:
```
Change MC32S advanced parameters?  (y/[n]) :
```

14 Enter:
```
y
```
The following prompt appears:
```
TLAN is set to auto negotiate, change?  (y/[n]) :
```

15 Enter:
```
n
```
The following prompt appears:
```
ELAN security Disabled, change?  (y/[n]) :
```

16 To enable ISSS/IPsec security, enter:
```
y
```
The following prompt appears:
```
Enable ELAN security ?  (y/[n]) :
```

17 Enter:
```
y
```
to enable ISSS. The following prompt appears:
```
Enter security level OPTI, FUNC or FULL:
```

18 Enter:
```
func
```
to select the FUNC (Functional) security level. The following

prompt appears:
`Change public key? (y/[n]) :`

ATTENTION
The IPsec key is not a public key, it is a secret preshared key.

19 To change the ISSS/IPsec preshared key (PSK), enter:
`y`
The following prompt appears:
`Note: Spaces ~ * ' @ [ ] and # are not supported in passwords.`
`Please input PSK(16-32 chars):`

20 Enter the IPsec PSK, which can be 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_-+={}|\:;"'<,>.?/. Do not use spaces in the key.
The following prompt appears:
`Please input PSK(16-32 chars):`

21 Reenter the IPsec PSK value.
The following prompt appears:
`Strength of PSK: <strength>` . The strength value that appears is one of Weak, Medium, or Strong. Nortel recommends that you use a strong key. If you are satisfied with the strength of the PSK, proceed to step 17.

22 To create a stronger PSK, enter the IPsec change PSK command:
`isecChgPSK`.
The following prompt appears:

`Are you sure you want to continue? (Yes/[No]):`

23 Enter **`yes`** to confirm that you want to change the IPsec PSK.

24 Enter the new IPsec PSK.

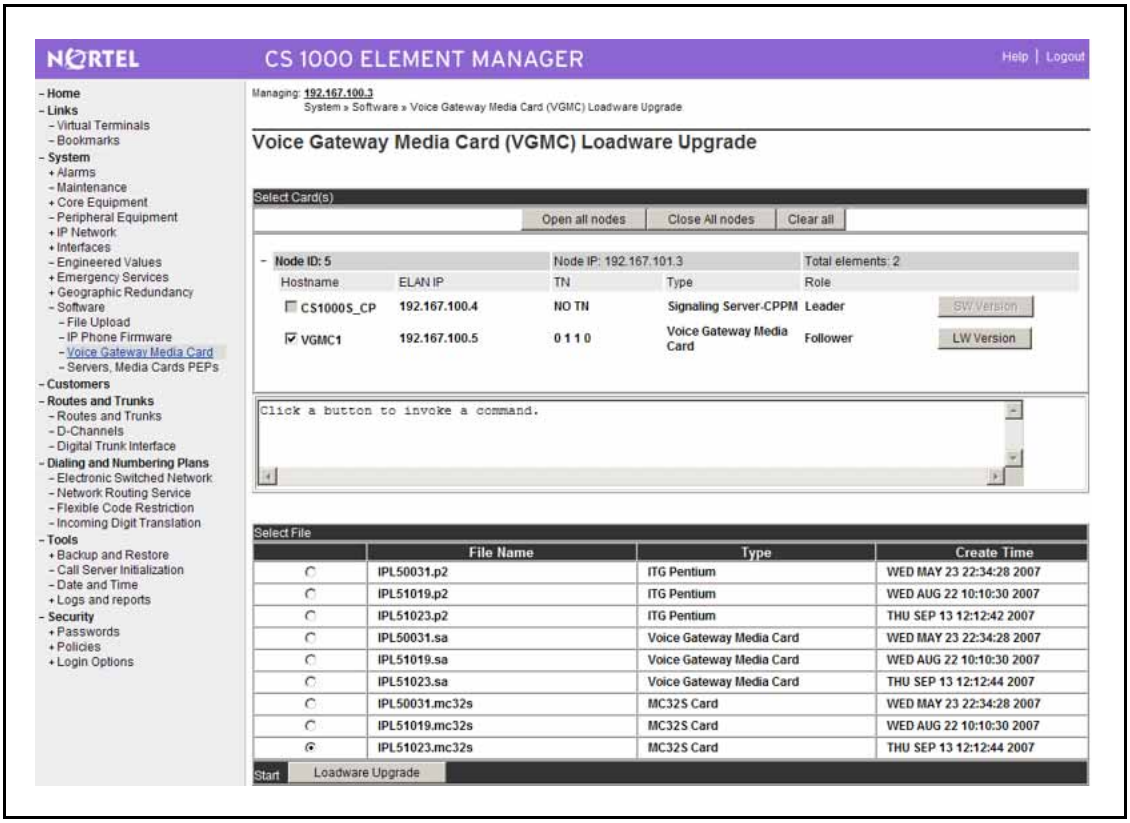
A prompt appears that requests confirmation of the new IPsec PSK.

25 Reenter the new PSK.

The device saves the IPsec PSK.

26 Log on to Element Manager on the Signaling Server you targeted in step 10.

27 Click **System** > **Software** > **Voice Gateway Media Card**.
The **Voice Gateway Media Card (VGMC) Loadware Upgrade** page appears.



28 In the **Select Card(s)** pane, expand the node of which the new MC32S is a part, and check the box next to the new MC32S.

29 In the **Select File** pane, check the box next to the most recent entry with the type MC32S Card.

30 Click **Loadware Upgrade**.
Wait one minute for the loadware to copy onto the new MC32S.

31 Log on to the CLI on the MC32S you are adding.

32 Enter:
`mc32ssetup`

The following prompt appears:
`Please define the data networking parameters for this MC32S now.`
`Hostname :`

33 Bypass each prompt by pressing:
Enter
until the following prompt appears:
`Leading Secondary CS IP:`

34 Enter the IP Address of the Leading Secondary Call Server. If you do not have a Leading Secondary Call Server, enter 0.0.0.0.

35 Bypass each remaining prompt by pressing:
Enter

until the new settings are listed, and following prompt appears:

```
Leading Secondary CS Hostname:
Is this correct?  (y / n /[a]bort):
```

36 Enter:

y

The following prompt appears:

```
The above changes require reboot to take effect.
Do you want to reboot now?  (y/n/[a]bort) :
```

37 Enter:

y

The card restarts.

38 Using the local serial port or SSH, log on to the shell of the new device (the IPL shell if you are adding or replacing a Voice Gateway Media Card, or the OAM shell if you are adding or replacing the Signaling Server).

39 Enter the IPsec new target command to create an IPsec target for the Call Server:

isecNewTarget <CALL SERVER ELNK ACTIVE IP>

40 Enter the enable IPsec target command:

isecEnlTarget <CALL SERVER ELNK ACTIVE IP>

41 Enter the IPsec new target command to create an IPsec target for local Element Manager :

isecNewTarget <local ELEMENT MANAGER ELAN IP>

42 Enter the enable IPsec target command:

isecEnlTarget <local ELEMENT MANAGER ELAN IP>

If you do not have remote centralized Element Manager on ECM, proceed to step 16.

43 Enter the IPsec new target command to create an IPsec target for the ELAN interface of the remote centralized Element Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER ELAN IP>

44 Enter the enable IPsec target command:

isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

45 Enter the IPsec new target command to create an IPsec target for the TLAN interface of the remote centralized Element Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER TLAN IP>

46 Enter the enable IPsec target command:

isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

47 Enter the change IPsec PSK command:

isecChgPSK

The following prompt appears:

```
Are you sure you want to continue?  (Yes/[No]):
```

48 Enter **yes** to confirm that you want to change the IPsec PSK.

49 Enter the new IPsec PSK.

Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key.

A prompt appears that requests confirmation of the new IPsec PSK.

50 Reenter the new PSK.

The device saves the IPsec PSK.

51 Enter the IPsec Change level command
isecChgLevel [OPTI/FUNC/FULL]

The following prompt appears: `Are you sure you want to continue?  (Yes/[No]):`

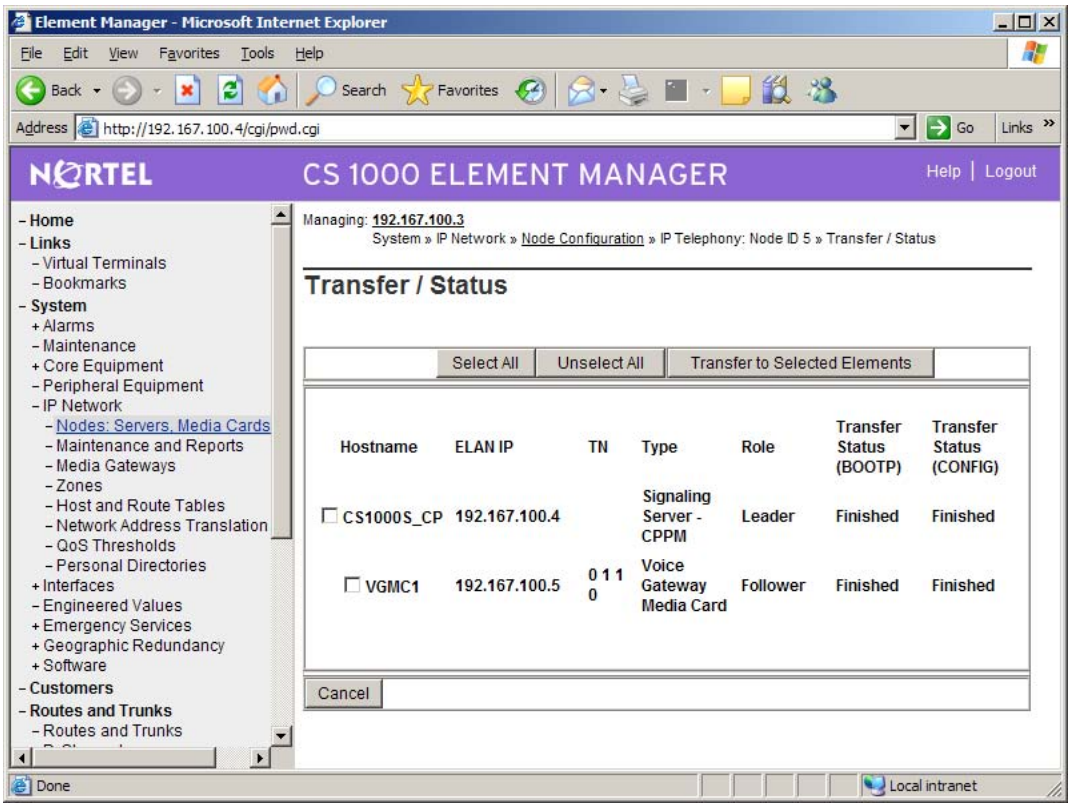
52 Enter:
yes
The ISSS security level is configured, and ISSS is enabled.

53 Enter the following command to ensure that the pbxLink with the new device is active:
pbxLinkShow
The pbxLink status appears.

54 Log on to Element Manager on the local Signaling Server that you targeted in step 10.

55 Click **System** > **IP Network** > **Nodes: Servers, Media Cards**.
The **Node Configuration** page appears.

56 Click **Transfer/Status** next to the node of which the new device is a part.
The **Transfer/Status** page appears.



57 Verify that the Transfer status columns contain a value of *Finished*.

58 Click **Security** > **Login Options** > **Intra Nodal Security** to return to the **Intra Nodal Security** page.

59 Click **Edit**.
The **Intra Nodal Security Configuration** page appears.

60 Disable and then reenable ISSS to send the current ISSS system status to the new device:
Clear the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.

Click **Edit** to return to the **Intra Nodal Security** page.
Check the **Enable Intra Nodal Security** check box.
Click **Save** to return to the **Intra Nodal Security** page.
Click **Commit** to transmit the ISSS target information.

--End--

Table 28
Variable definitions

Variable	Value
<CALL SERVER ELNK ACTIVE IP>	The ELNK ACTIVE IP address of the call server.
<local ELEMENT MANAGER ELAN IP>	The ELAN IP address of a local Element Manager Signalling Server host that is in the same IP telephony node as the new device[1].
<remote ELEMENT MANAGER ELAN IP>	The ELAN IP address of remote centralized Element Manager.
<remote ELEMENT MANAGER ELAN IP>	The TLAN IP address of remote centralized Element Manager.

Use the following procedure to add an MGC when ISSS is enabled.

Procedure 9
Adding an MGC when ISSS is enabled

Step	Action
1	Log on to the CLI on the MGC you are adding.

2	Enter:
	mgcsetup
	The following prompt appears:
	`Bootline stored in NV_RAM`
	`Change MGC advanced parameters? (y/[n]) :`

3	Enter:
	`y`
	The following prompt appears:
	`TLAN is set to <TLAN option>, change? (y/[n]) :`

4	Enter:
	`n`
	The following prompt appears:
	`ELAN is set to <ELAN option>, change? (y/[n]) :`

5	Enter:
	`y`
	The following prompt appears:
	`ELAN security Disabled, change? (y/[n]) :`

6	To enable ISSS/IPsec security, enter:
	`y`
	The following prompt appears:
	`Enable ELAN security ? (y/[n]) :`

7	Enter: `y` To change the ISSS security level. The following prompt

appears:
```
Enter security level OPTI, FUNC or FULL :
```

8 Enter:
```
func
```
to select the FUNC (Functional) security level. The following prompt appears:
```
Change public key?  (y/[n]) :
```

ATTENTION
The IPsec key is not a public key, it is a secret preshared key.

9 To change the ISSS/IPsec preshared key (PSK), enter:
```
y
```
The following prompt appears:
```
Note:  Spaces ~ * ' @ [ ] and # are not supported in
passwords.
Please input PSK(16-32 chars):
```

10 Enter the IPsec PSK, which can be 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_-+={}|\:;"'<,>.?/. Do not use spaces in the key.
The following prompt appears:
```
Strength of PSK: <strength>
Please input PSK(16-32 chars):
```
. The strength value that appears is one of Weak, Medium, or Strong. Nortel recommends that you use a strong key.

11 Reenter the IPsec PSK.
The following message and prompt appears:
```
You have entered the following parameters for this
MGC:
ELAN IP: <ELAN IP>
ELAN subnet mask:  <ELAN subnet mask>
ELAN gateway IP <ELAN gateway IP>
Primary CS IP: <primary Call Server IP>
TLAN set to auto-negotiate
ELAN set to auto-negotiate
ELAN security Enabled, level is Functional Security
Is this correct?  (y/n/[a]bort):
```

12 Enter **y**.
The following message appears:
```
The above changes require Reboot to take effect.
Do you want to reboot now?  (y/n/[a]bort):
```

13 Enter **y** to restart the new MGC.

14 Log on to the CLI on the MGC.

15 If you are satisfied with the strength of the PSK, proceed to step 17. To create a stronger PSK, enter the IPsec change PSK command:

isecChgPSK.
The following prompt appears:

```
Are you sure you want to continue?  (Yes/[No]):
```

16 Enter **yes** to confirm that you want to change the IPsec PSK.

17 Enter the new IPsec PSK.

A prompt appears that requests confirmation of the new IPsec PSK.

18 Reenter the new PSK.

The device saves the IPsec PSK.

19 Enter the IPsec new target command to create an IPsec target for local Element Manager :
isecNewTarget <local ELEMENT MANAGER ELAN IP>

20 Enter the enable IPsec target command:
isecEnlTarget <local ELEMENT MANAGER ELAN IP>
If you do not have remote centralized Element Manager on ECM, proceed to step 28.

21 Enter the IPsec new target command to create an IPsec target for the ELAN interface of the remote centralized Element Manager on ECM:
isecNewTarget <remote ELEMENT MANAGER ELAN IP>

22 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER ELAN IP>

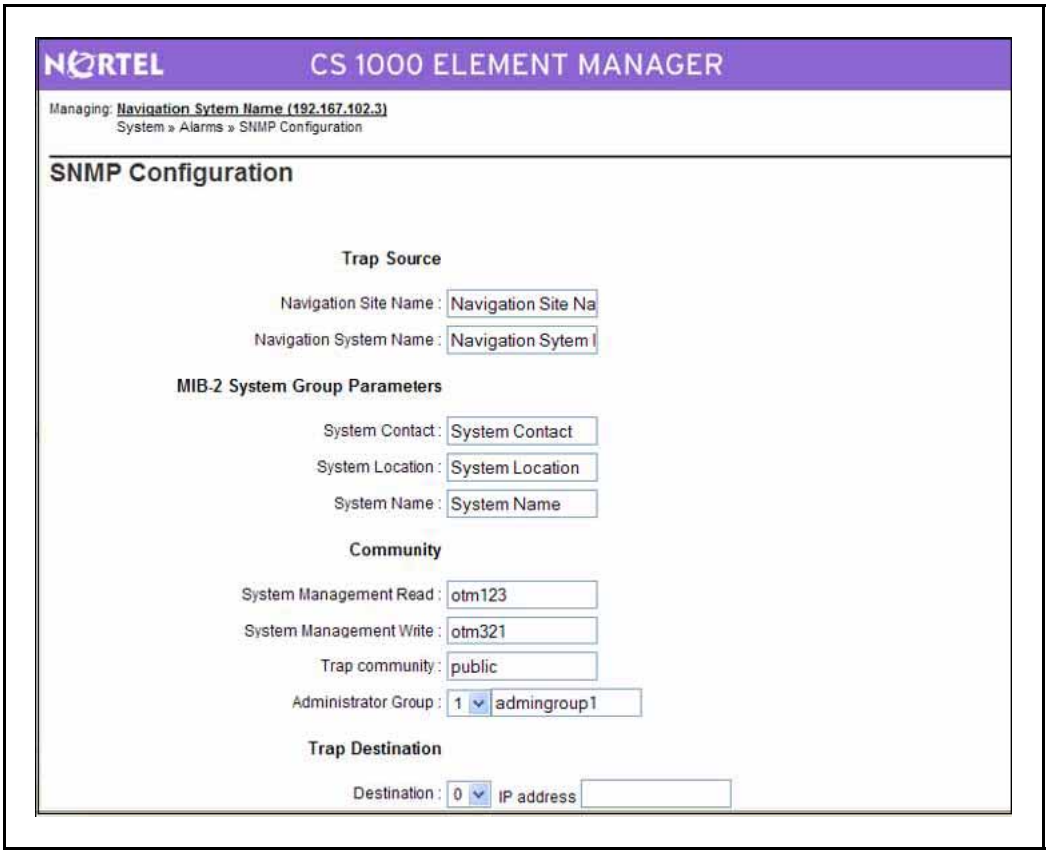
23 Enter the IPsec new target command to create an IPsec target for the TLAN interface of the remote centralized Element Manager on ECM:

isecNewTarget <remote ELEMENT MANAGER TLAN IP>

24 Enter the enable IPsec target command:
isecEnlTarget <remote ELEMENT MANAGER TLAN IP>

25 Log on to Element Manager on the local Signaling Server using a System password level 2 account.

26 Click **System** > **Alarms** > **SNMP**.
The **SNMP Configuration** page appears.



27 In the **Destination** field, select a trap destination number.

28 In the **IP Address** field, enter the IP address of the Signaling Server you use for system configuration and management.

29 Click **Save**.

30 Log on to the call server using a PWD2 account.

31 At the LD 43 prompt, enter
EDD
An Equipment Data Dump (EDD) occurs, and host route entries for new trap destinations are added to the network routing table for the Signaling Server, Voice Gateway Media Cards, and MGCs.

32 Restart the new MGC.

--End--

Table 29
Variable definitions

Variable	Value
<ELAN Option>	One of auto-negotiate or full-duplex.

Table 29
Variable definitions (cont'd.)

Variable	Value
<local ELEMENT MANAGER ELAN IP>	The ELAN IP address of a local Element Manager Signalling Server host that is in the same IP telephony node as the new device[1].
<remote ELEMENT MANAGER ELAN IP>	The ELAN IP address of remote centralized Element Manager.
<remote ELEMENT MANAGER TLAN IP>	The TLAN IP address of remote centralized Element Manager.
<TLAN Option>	One of auto-negotiate or full-duplex.

Other ISSS configuration and maintenance procedures

This section contains ISSS/IPsec maintenance and configuration procedures. Instead of using the information in this section to configure ISSS/IPsec for the first time, or to add, remove, or replace system components when ISSS is configured and enabled, see the following sections:

- "First-time configuration and activation of ISSS" (page 48)
- "Add, remove, or replace a CS 1000 system element when ISSS is enabled and active" (page 68)

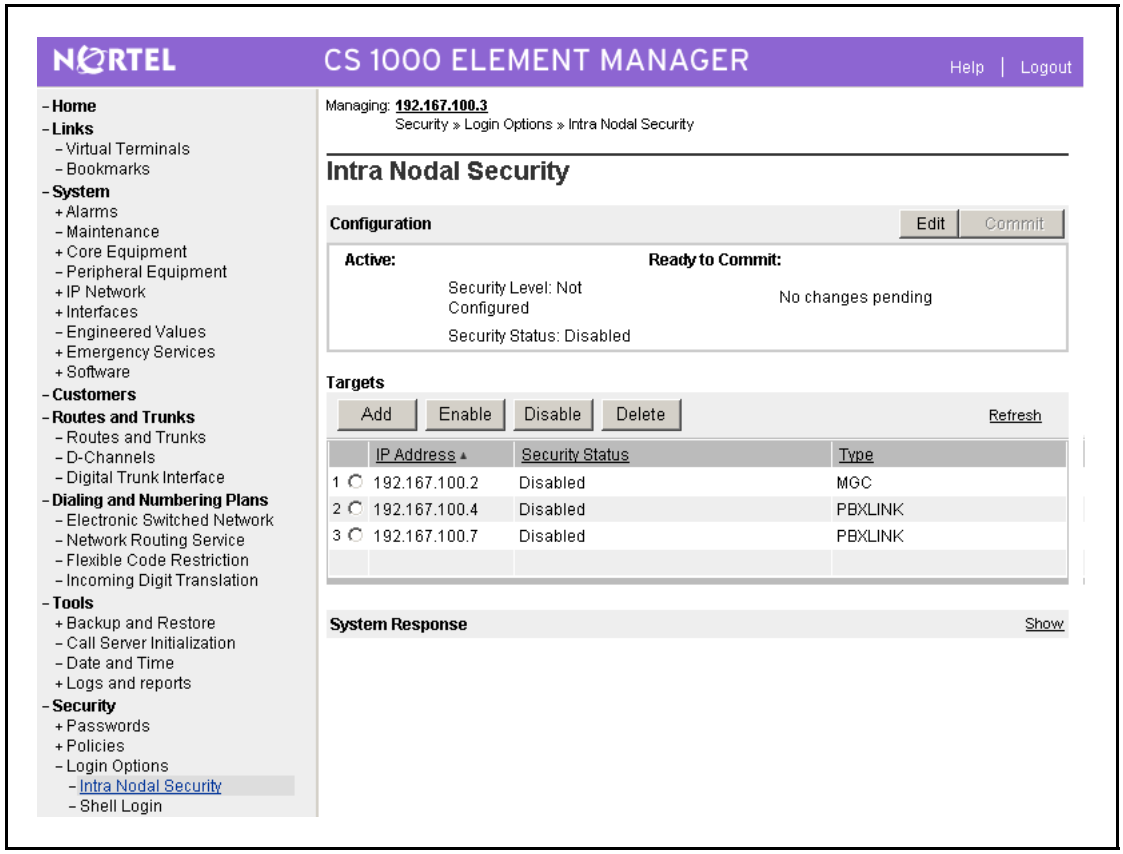
For all other ISSS/IPsec configuration and maintenance, use the procedures in this section.

ISSS configuration using Element Manager

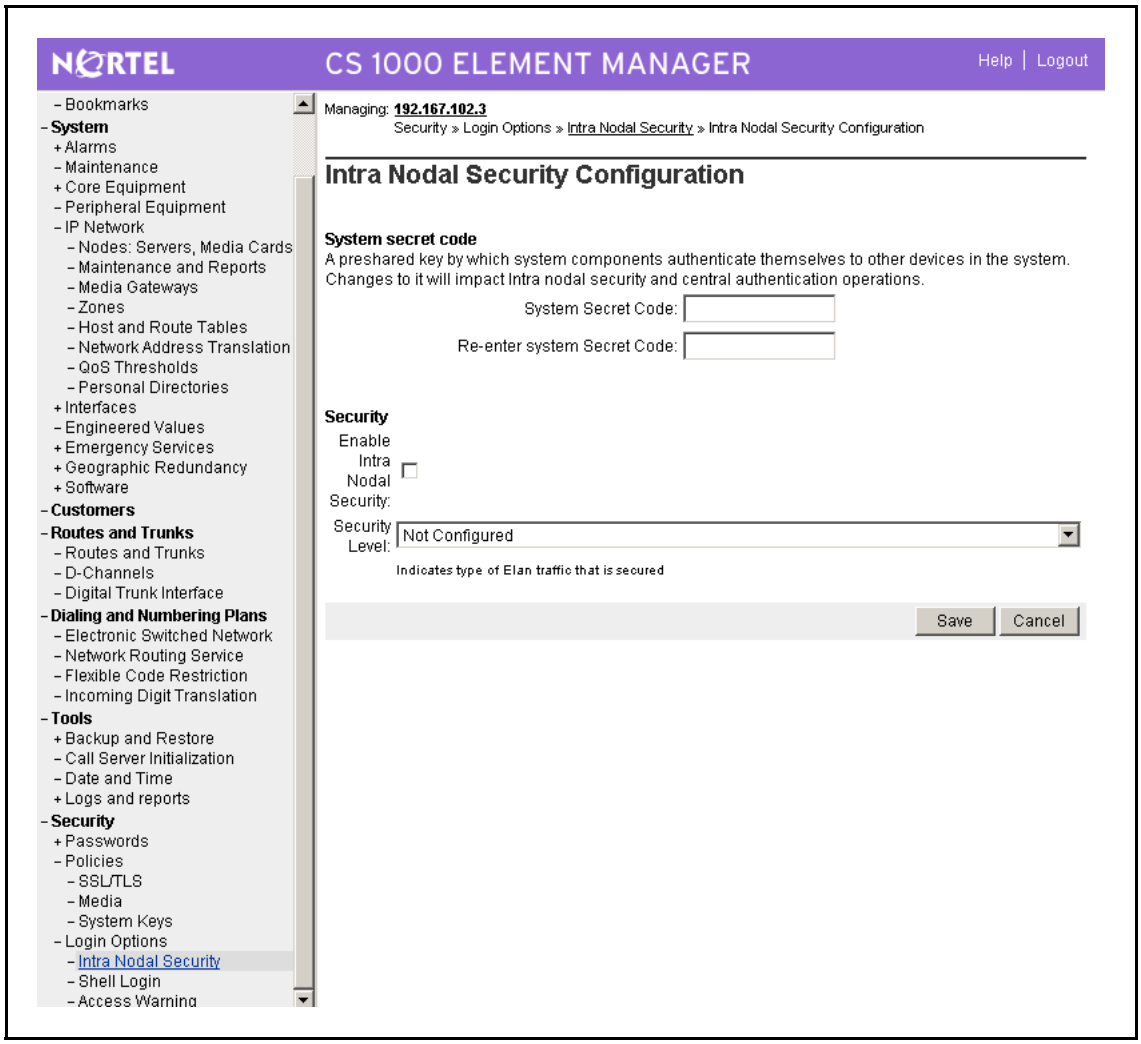
Use the following procedure to configure ISSS options, change security status, or change the System IPsec PSK, using Element Manager.

Procedure 10
Configuring ISSS options by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Intra Nodal Security**. The **Intra Nodal Security** page appears.



3 Click **Edit**.
The **Intra Nodal Security Configuration** page appears.

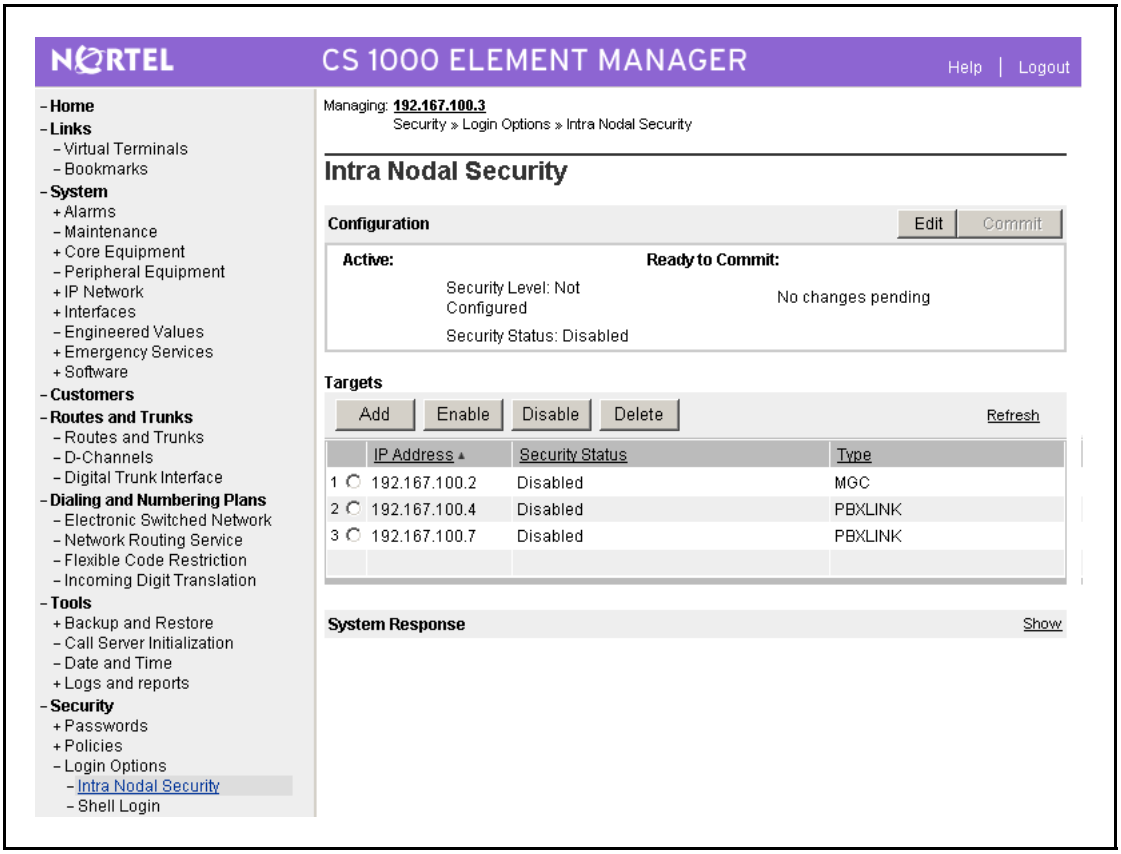


4 Configure the following options:

- Enter a new system IPsec PSK **System Secret Code** field.
- Reenter the IPsec PSK in the **Re-enter system Secret Code** to confirm the new value.
- Select or clear **Enable Intra Nodal Security** to enable or disable ISSS/IPsec.
- From the **Security Level** list, choose **Optimized**, **Functional**, or **Full**.

5 Click **Save**.

The **Intra Nodal Security** page appears.



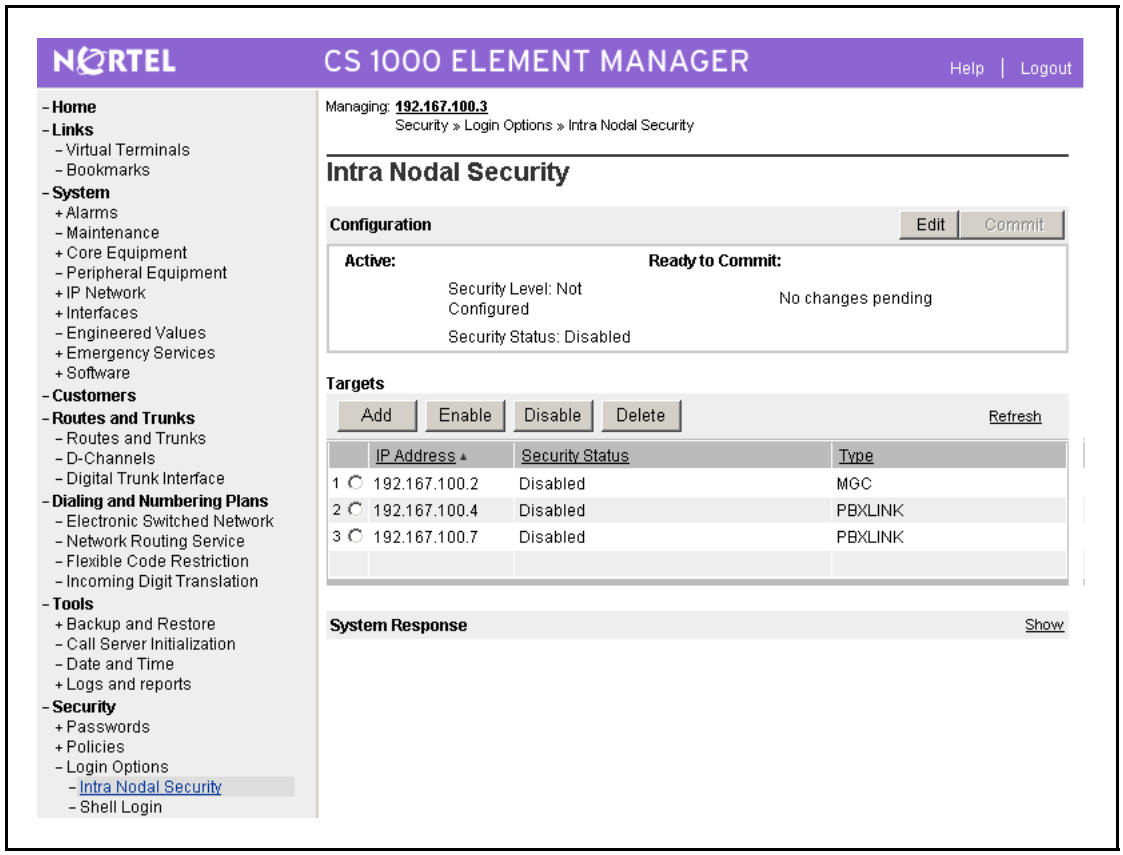
6 Click **Commit** to commit your changes to the system.

--End--

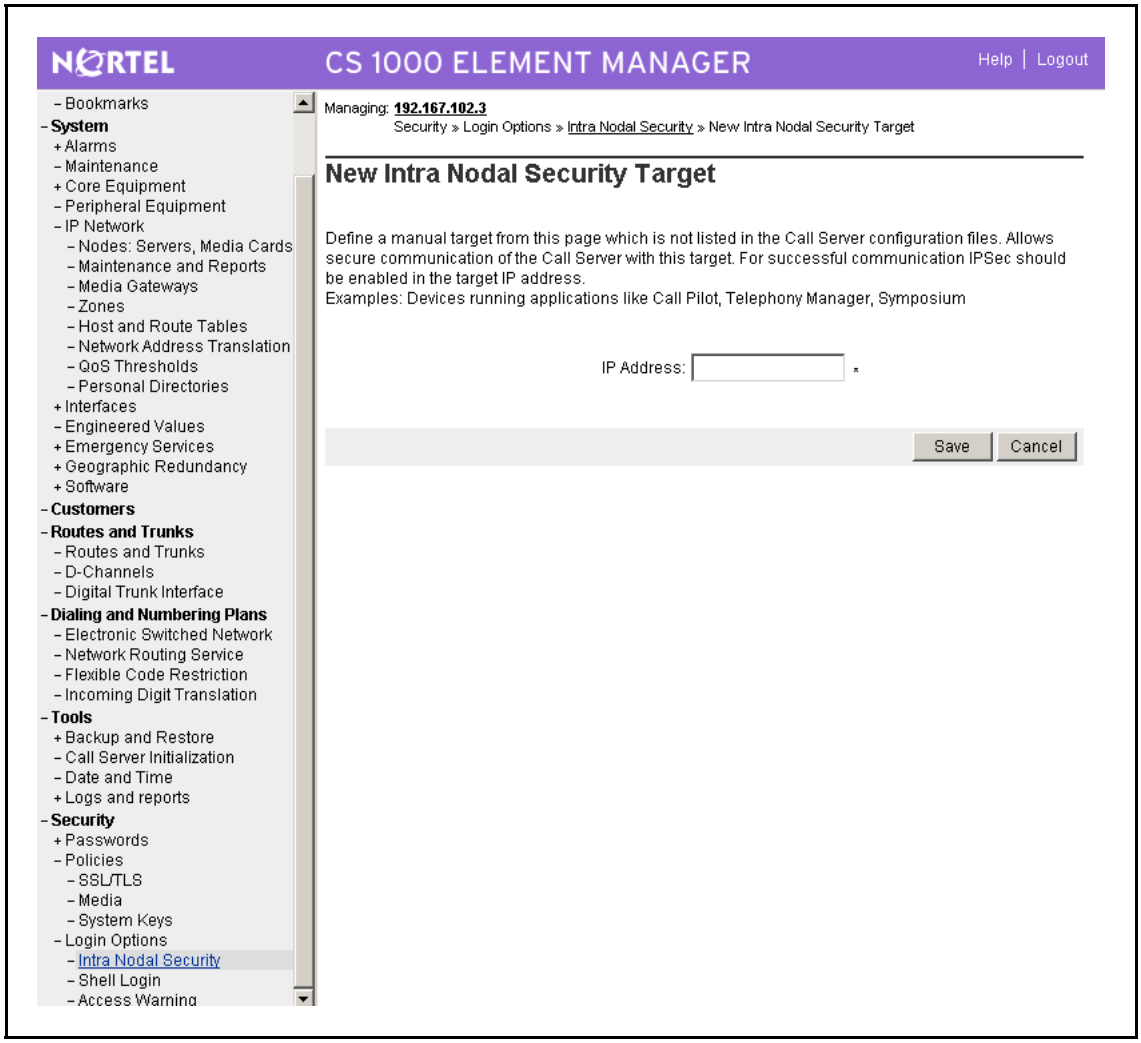
Use the following procedure to manually add a target in Element Manager.

Procedure 11
Adding an ISSS target manually by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Intra Nodal Security** . The **Intra Nodal Security** page appears.



3 Click **Add**.
The **New Intra Nodal Security Target** page appears.



4 Enter the IP Address for the new target.

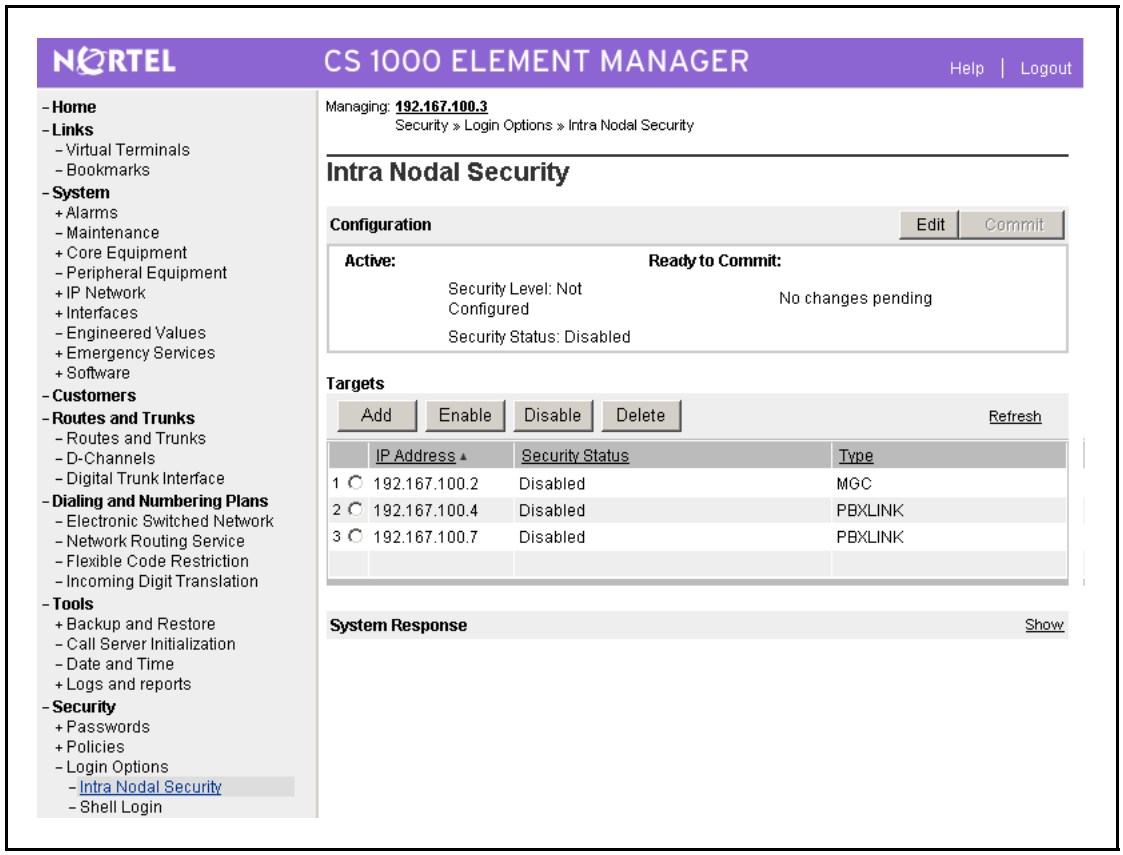
5 Click **Save**.

--End--

Use the following procedure to enable, disable, or delete a target.

Procedure 12
Enabling or disabling an existing ISSS target by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Intra Nodal Security**. The **Intra Nodal Security** page appears.



3 Select the check box next to the entry you want to enable or disable.

4 Click **Enable** or **Disable**.

A confirmation requester appears.

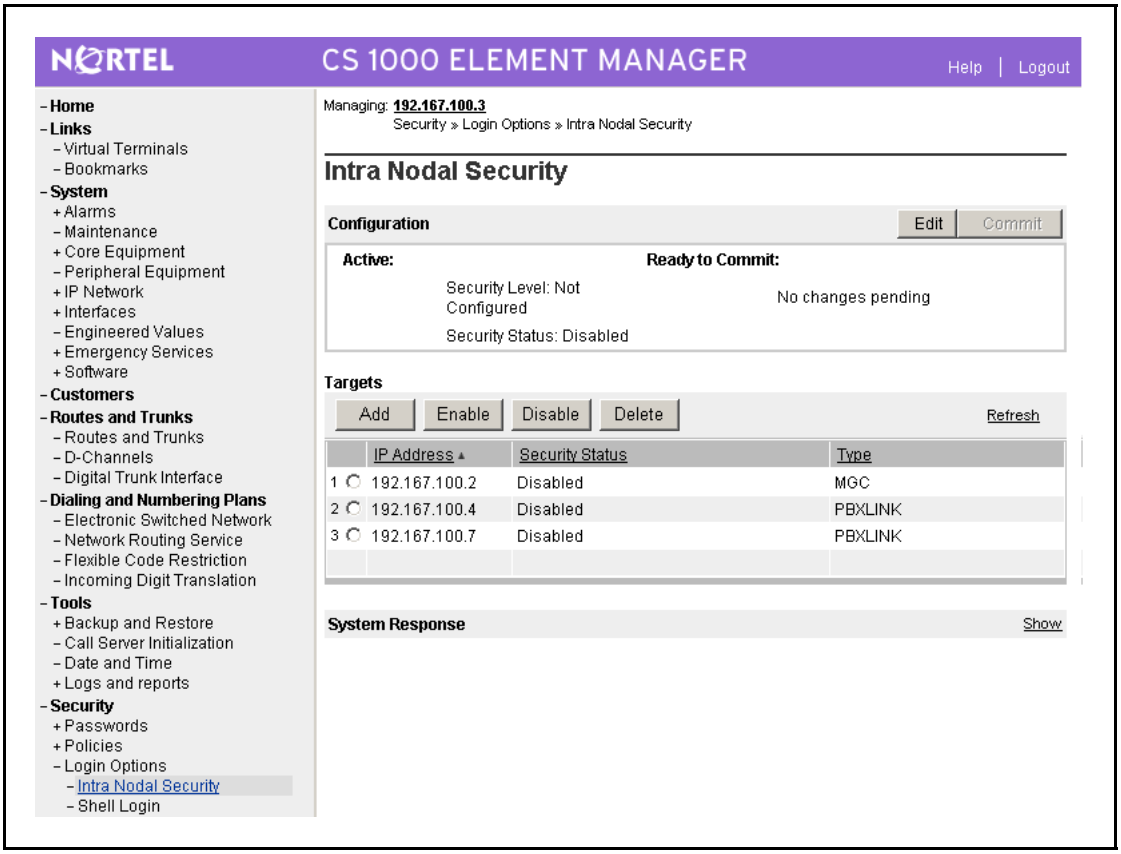
5 Click **OK**.

--End--

Use the following procedure to delete an ISSS target.

Procedure 13
Deleting an ISSS target by using Element Manager

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Login Options > Intra Nodal Security** . The **Intra Nodal Security** page appears.



3 Select the option button next to the entry you want to delete.

4 Click **Delete**.
A confirmation requester appears.

5 Click **OK** to delete the target.

--End--

Nortel recommends that, instead of using the procedures in this section, you configure ISSS for the first time using the procedures in "Recommended methods for first-time ISSS configuration" (page 49). The procedures in this section are provided as an alternative in case you cannot use the recommended methods.

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.

Use the following procedure to configure ISSS for the first time using overlays.

ISSS configuration from the call server using overlays

This section describes commands you can use to configure system-wide ISSS settings using overlays.

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.

Use the following procedure to change the system IPsec PSK.

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 14
Changing the IPsec PSK by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **`CHG ISEC PSK`**. A prompt appears that requests the new IPsec PSK.
3	Enter the new IPsec PSK. Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key. After you enter the new key, the system subjects it to strong password checking, and the strength of the IPsec PSK appears (Weak/Medium/Strong). You can optionally reenter the change key command, and enter a stronger key. A prompt appears, requesting confirmation of the new IPsec PSK.
4	Reenter the new IPsec PSK. The system sends a message to all connected devices indicating that the IPsec PSK has changed, and each device returns a message acknowledging that the new IPsec PSK is received. After acknowledgement is received from all connected devices, the system saves the new IPsec PSK locally.
5	After the connected devices acknowledge the change, complete any other ISSS configuration before configuring the ISSS level.

--End--

ATTENTION
If you are using ECM to manage more than one system, each system must use the same IPsec PSK as ECM or traffic is not ISSS encrypted.

Use the following procedure to configure the ISSS security option, which enables ISSS and determines which links are encrypted.

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 15
Changing the ISSS/IPsec security level by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: `CHG ISEC {OPTI | FUNC | FULL}` The system sends a message to all connected devices indicating the change. The connected devices acknowledge the change.

--End--

Table 30
Job aid: ISSS/IPsec security levels

ISSS/IPsec security level	Description
Optimized Security	(OPTI) Traffic over pbxLink and Xmsg between this host and its IPsec targets[1] is protected by IPsec. Any other traffic (other than pbxLink or Xmsg) between this host and its IPsec targets is permitted, but is NOT protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.
Functional Security	(FUNC) All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, but is NOT protected by IPsec.

Table 30
Job aid: ISSS/IPsec security levels (cont'd.)

Full Security	(FULL)[3] All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is NOT permitted, except BootP, SSH (port 22), SSL (port 443), NTP (port 123), and AML (port 888). To connect with Element Manager on a signaling server over the ELAN when ISSS security policy Full is used, you must use HTTPS (HTTPS uses SSL).
Note[1] IPsec targets are either internal IPsec targets are that are added automatically when certain devices read IP addresses from a system configuration file and create IPsec targets for them, or external IPsec targets that are added from the command line. Note[2] ISSS neither blocks nor encrypts connections through the TLAN subnet. For VxWorks based hosts (Signaling Server, MGC, Voice Gateway Media Card), all traffic over the TLAN subnet is accepted over IP and is not encrypted. Note[3] ISSS security policy FULL is not available on the ECM host. If you configure the CS 1000 System to use ISSS security policy Full, configure the ECM to use ISSS security policy FUNC.	

Use the following procedure to enable ISSS for the entire 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**.

Procedure 16
Enabling ISSS by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **`ENL ISEC`** The system sends the updated status to all connected devices. The connected devices acknowledge the change.

--End--

Use the following procedure to disable ISSS for the entire 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**.

Procedure 17
Disabling ISSS by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **DIS ISEC** The system sends the updated status to all connected devices. The connected devices acknowledge the change.

--End--

Use the following procedure to view information about ISSS configuration.

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 18
Viewing ISSS information by 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 ISEC {ALL | EXCEP | TARGET | SYNC}**

--End--

Table 31
Variable definitions

Variable	Value
ALL	Prints all ISSS related information, including a summary of ISEC and target list.
EXCEP	Prints a summary of ISSS and exception list.
TARGET	Prints a summary of ISSS and manually configured target list
SYNC	Prints a summary of ISSS and all targets synchronization status.
No parameter	Prints a summary of system ISSS information.

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 19
Committing changes to ISSS configuration by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	Optionally, at the LD 117 prompt, enter: **PRT ISEC** to verify IPsec/ISSS configuration before committing changes.

3	At the LD 117 prompt, enter: **commit isec**
	The following message appears:
	`=> commit isec`
	`PSK has been synchronized`
	`Security Level has been synchronized`
	`Security Status has been synchronized`
	
	`------------------------Target synchronization Information----------------------`
	`IPAddr Type PSKSync LevelSync statusSync LinkStatus`
	`-------------------------------------------------`
	`192.167.104.54 PBXLINK ReceivedACK ReceivedACK ReceivedACK LinkUp`
	`192.167.104.52 MGC ReceivedACK ReceivedACK ReceivedACK LinkUp`
	
	`This change will affect ELAN operations.`
	`Are you sure you want to continue this process? (Yes/[No])`

4	Enter **yes** or **no** .

--End--

Configure ISSS targets using overlays

Use the procedures in this section to define, remove, enable and disable an individual IPsec target for the entire system. You must create targets for IP telephony system elements that are managed through Element Manager.

Create targets for:

- Element Manager on ECM
- Certificate management on NRS
- Geographic Redundancy on secondary call servers

Do not create targets for elements that are defined in the IP telephony nodes, (including the local call server and MGC). If the system is the primary Geographic Redundancy server, then you need to add the following targets for the call server:

- Media Gateway Controller (MGC)
- Voice Gateway Media Card
- Call server
- Signaling Server

Use the following procedure to manually create, enable, and add a target to the trusted host list.

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 20
Creating an ISSS target by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **NEW ISECTAR <target IP>**.

--End--

Use the following procedure to disable a target, but leave it defined as an IPsec target.

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 21
Disabling an ISSS target by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **DIS ISECTAR <target IP>**

to disable the Intrasystem Signaling Security feature for a given target for the entire system.

--End--

Use the following procedure to enable a target that was previously 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 22
Enabling an ISSS target by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **`ENL ISECTAR <target IP>`** to enable the Intrasystem Signaling Security feature for a given target for the entire system.

--End--

Use the following procedure to manually delete a target.

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 23
Deleting an ISSS target by using LD 117

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **`OUT ISECTAR <target IP>`**.

--End--

Use the following procedure to view information about manually configured targets.

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 24
Viewing manually configured ISSS targets by 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 ISECTAR** Information about manually configured ISSS targets appear.

--End--

Prerequisites

- Ensure that all system elements (Signaling Servers, MGCs, and Voice Gateway Media Cards) are registered with the call server.

Use the following procedure to configure ISSS for the first time using overlays.

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 25
Configuring ISSS for the first time using overlays

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	Enter the change key command at the LD 117 prompt: **CHG ISEC PSK**. A prompt appears to request the new IPsec PSK.
3	Enter the new IPsec PSK. Enter a key of 16 to 32 characters, using any of the following characters: 0 to 9, A to Z, a to z, !$%^&()_- +={}|\:;"'<,>.?/. Do not use spaces in the key. After you enter the new key, the system subjects it to strong password checking and the strength of the IPsec PSK appears (Weak/Medium/Strong). You can optionally reenter the change key command and enter a stronger key. A prompt appears to confirm the new IPsec PSK.

4 Reenter the new IPsec PSK.

The system sends a message to all connected devices to indicate that the IPsec PSK is changed, and each device returns a message that acknowledges the new IPsec PSK. After all connected devices send acknowledgement, the system saves the new IPsec PSK locally.

5 Enter the change IPsec level command at the LD 117 prompt:
CHG ISEC {OPTI | FUNC | FULL}

The system changes the ISSS security level and sends a message to all connected devices to indicate the change.

6 Enter the enable IPsec command at the LD 117 prompt:
ENL ISEC

The system enables ISSS, and sends the updated status to all connected devices.

7 Enter the commit IPsec command at the LD 117 prompt:
commit isec

The following output appears:

```
=> commit isec
PSK has been synchronized
Security Level has been synchronized
Security Status has been synchronized

------------------------Target synchronization
Information----------------------
IPAddr Type PSKSync LevelSync statusSync
LinkStatus
-----------------------------------------------
-
192.167.104.54 PBXLINK ReceivedACK ReceivedACK
ReceivedACK LinkUp
192.167.104.52 MGC ReceivedACK ReceivedACK
ReceivedACK LinkUp

This change will affect ELAN operations.
Are you sure you want to continue this process?
(Yes/[No])
```

8 Enter:

yes
to commit changes.

--End--

Procedure 26
Configuring ISSS on ECM using the CLI

Step	Action
1	Log on to the ECM CLI using the log on name nortel.
2	Add the PSK on each CS 1000 system by entering the following command for each one: **`newipsectarget <CS 1000 IP address> <IPsec PSK> <ISSS level>`** A prompt appears requesting that you enter the root password.
3	Enter the root password.
4	Configure the ISSS level on each signaling server by entering the following command for each one: **`newipsectarget <Signaling Server IP address> <IPsec PSK> <ISSS level>`** The Signaling Server target is added, and keys are exchanged. A prompt appears requesting that you enter the root password.
5	Enter the root password.

--End--

Table 32
Variable definitions

Variable	Value
<CS 1000 IP address>	The IP address of the CS 1000 system to configure as an IPsec target.
<ISSS level>	The ISSS level, which must be either OPTI or FUNC.
<IPsec PSK>	The IPsec PSK.
<Signaling Server IP address>	The IP address of the Signaling Server to configure as an IPsec target.

Add a VxWorks element to a CS 1000 domain

Use the following procedure to add a new VxWorks system element to a CS 1000 domain where IPsec is already enabled. To do so, you must add the target on the call server, and then add the target on the Linux 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 27
Adding a VxWorks element to a CS 1000 domain when IPsec is enabled

Step	Action
1	Log on to the call server CLI using a PWD2 account.
2	At the LD 117 prompt, enter: **`NEW ISECTAR <target IP>`**.
3	Use an SSH or serial port console to log on to the Linux CLI using the log on name nortel.
4	Enter **`newipsectarget <IP address> <IPsec PSK> <sec level>`**. A prompt appears requesting that you enter the root password.
5	Enter the root password.

--End--

Table 33
Variable definitions

Variable	Value
<IPsec PSK>	The IPsec PSK.
<IP address>	The IP address of the element to be added
<ISSS level>	The ISSS level, which must be either OPTI or FUNC.
<target IP>	the IP address of the element to be added

Table 34
Job aid: ISSS/IPsec security levels

ISSS/IPsec security level	Description
Optimized Security	(OPTI) Traffic over pbxLink and Xmsg between this host and its IPsec targets[1] is protected by IPsec. Any other traffic (other than pbxLink nor Xmsg) between this host and its IPsec targets is permitted, and is NOT protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, and is NOT protected by IPsec.

Table 34
Job aid: ISSS/IPsec security levels (cont'd.)

Functional Security	(FUNC) All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is permitted, and is NOT protected by IPsec.
Full Security	(FULL)[3] All traffic (except BOOTP) between this host and its IPsec targets is protected by IPsec. All traffic between this host and any other host that is not defined as an IPsec target is NOT permitted, except BootP, SSH (port 22), SSL (port 443), NTP (port 123), and AML (port 888). To connect with Element Manager on a signaling server over the ELAN when ISSS security policy Full is used, you must use HTTPS (HTTPS uses SSL).
Note[1] IPsec targets are either internal IPsec targets are that are added automatically when certain devices read IP addresses from a system configuration file and create IPsec targets for them, or external IPsec targets that are added from the command line. Note[2] ISSS neither blocks nor encrypts connections through the TLAN subnet. For VxWorks based hosts (Signaling Server, MGC, Voice Gateway Media Card), all traffic over the TLAN subnet is accepted over IP and is not encrypted. Note[3] ISSS security policy FULL is not available on the ECM host. If you configure the CS 1000 System to use ISSS security policy Full, configure the ECM to use ISSS security policy FUNC.	

Remove a VxWorks element from a CS 1000 domain

Use the following procedure to remove a VxWorks system element from a CS 1000 domain where IPsec is enabled. To do so, you must remove the target from the call server, and then remove the target from the Linux 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 28
Removing a VxWorks element from a CS 1000 domain

Step	Action
1	Log on to the call server CLI using a PWD2 account.

2 At the LD 117 prompt, enter: **OUT ISECTAR <IP address>**, where <IP address> is the IP address of the element to be removed.

3 Use an SSH or serial port console to log on to the Linux CLI using the user name nortel.

4 Enter **removeipsectarget <IP address>**.
A prompt appears requesting that you enter the root password.

5 Enter the root password.

--End--

Table 35
Variable definitions

Variable	Value
<IP address>	The IP address of the element to be removed

Maintenance on Linux servers

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

Change ISSS/IPsec PSK on ECM 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 29
Changing the ISSS/IPsec PSK on ECM 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 36
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 30
Viewing IPsec target configurations for ECM 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` .

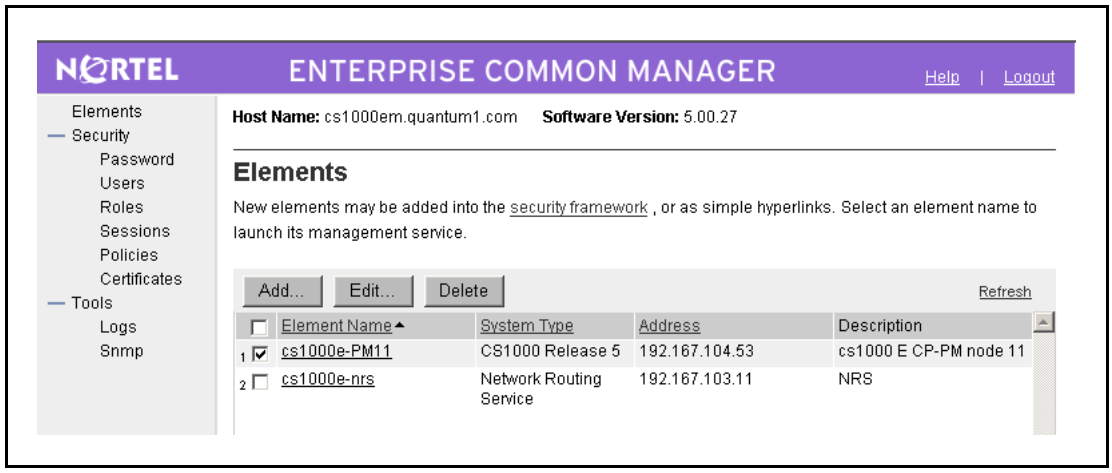
--End--

Change the IPsec PSK on ECM Linux host using Element Manager

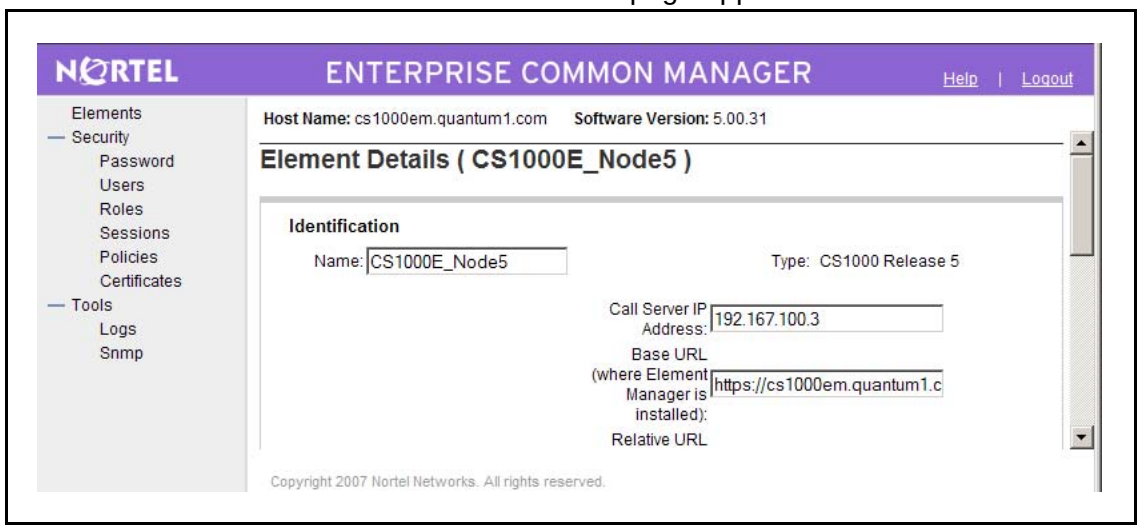
If you change the IPsec PSK on the call server, you must also change it on the ECM Linux host with Element Manager. For information about changing the IPsec PSK on the call server, see Procedure 14 “Changing the IPsec PSK by using LD 117” (page 104).

Procedure 31
Changing the ISSS/IPsec PSK for an IPsec Target that is a CS 1000 component on ECM Linux host using Element Manager

Step	Action
1	Log on to ECM using an account that has the SecurityAdministrator 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.



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



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 ECM, so they can encrypt traffic using ISSS.

Procedure 32
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 37
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 Enterprise Common Manager (ECM).

Procedure 33
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/FUNC/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 Enterprise Common Manager (ECM).

Procedure 34
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 Enterprise Common Manager (ECM).

Procedure 35
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 Procedure 114 “Confirming IPsec system settings on the active call server by using CLI or LD 117” (page 286).

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) and Transport Layer Security for Session Initiation Protocol (SIP TLS). The chapter is divided into the following sections:

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

For more information about public-key and private-key certificate concepts, Web SSL, and SIP TLS on Communication Server 1000 (CS 1000), see "Public-key certificate concepts" (page 36).

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 *Enterprise Common Manager Fundamentals (NN43001-116)* () .

Prepare the system for certificate management

The certificate management procedures in this chapter are performed on CS 1000 system elements. To manage certificates or certificate authorities (CA) for elements that do not yet exist, use the procedures in "Recommended methods for first-time ISSS configuration" (page 49) to add the elements to the list of system elements.

Nortel recommends that you perform certificate management from the ECM Primary security server that is running Element Manager. For certificate management purposes, the ECM element management table must contain an entry for each CS 1000 system and Signaling Server. You must add the CS 1000 elements and configure ISSS before you perform certificate management. For more information about adding system elements and configuring ISSS, see "Recommended methods for first-time ISSS configuration" (page 49). You must also add each CS 1000 system to the ECM 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 CS 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.

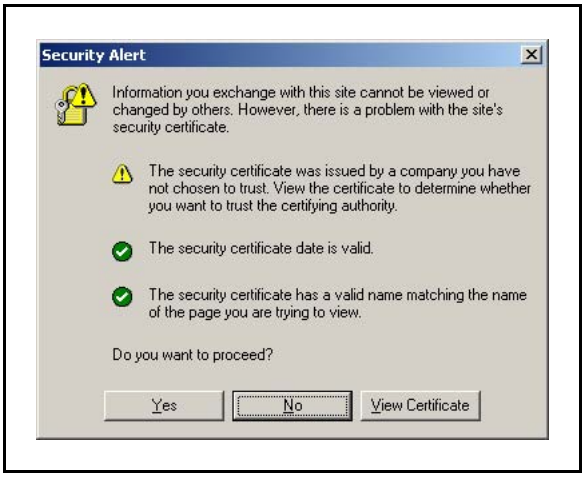
For more information about installing the CS 1000 applications, including the procedure for creating a private CA and configuring SSH trust, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)* () .

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 ECM Web server, the Sun Access Manager Web server, and the LDAP server.

Use the following procedure to access the primary security server.

Procedure 36
Accessing ECM 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.



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 38 “Install a certificate into the trusted CA list in the Web browser” (page 126).

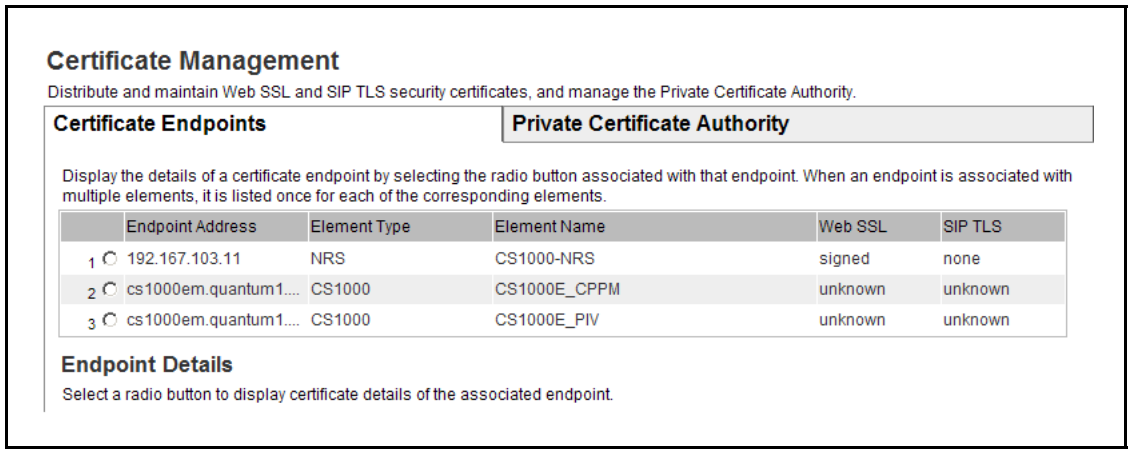
3 Click **Yes** to proceed.

--End--

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

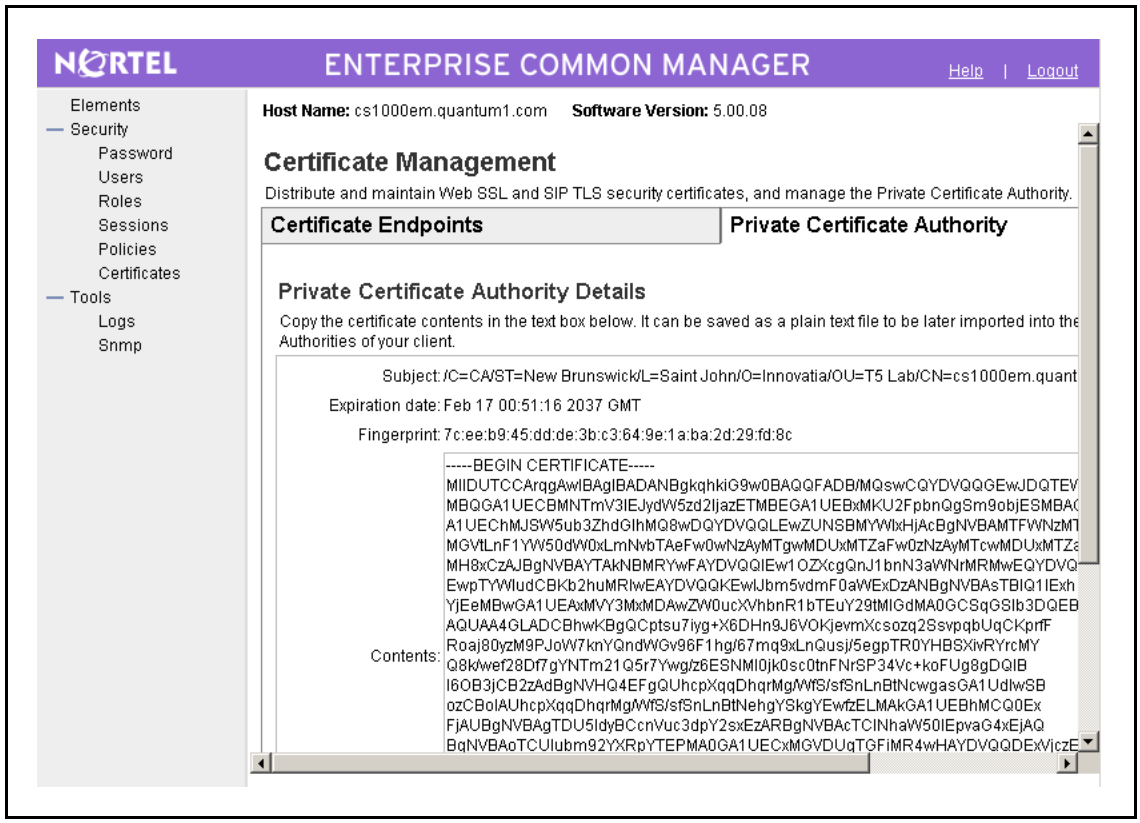
Procedure 37
Viewing private CA details

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



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

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

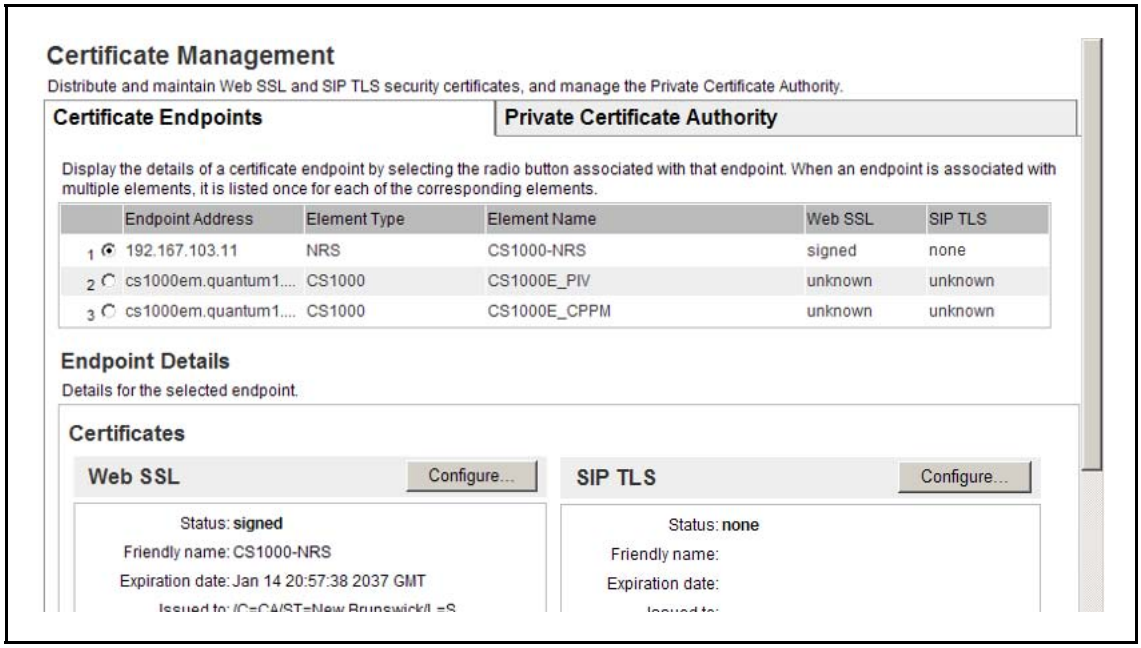


--End--

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

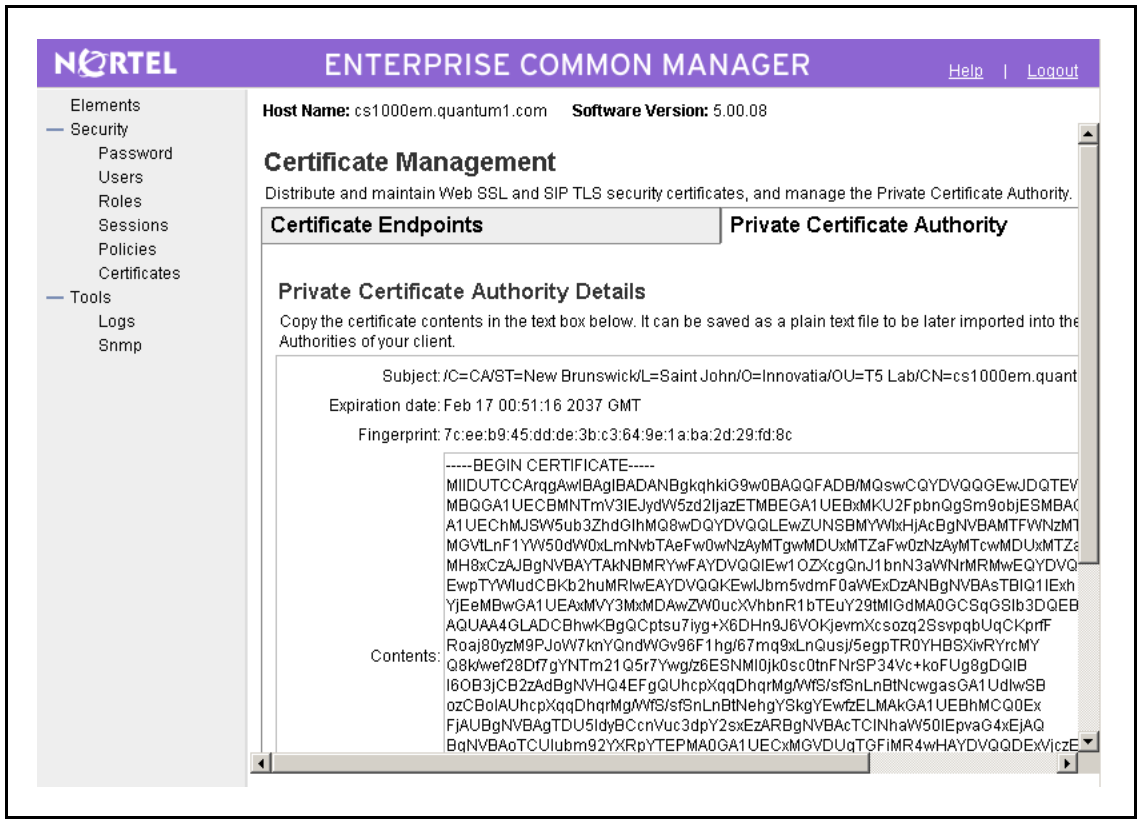
Procedure 38
Install a certificate into the trusted CA list in the Web browser

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



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

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

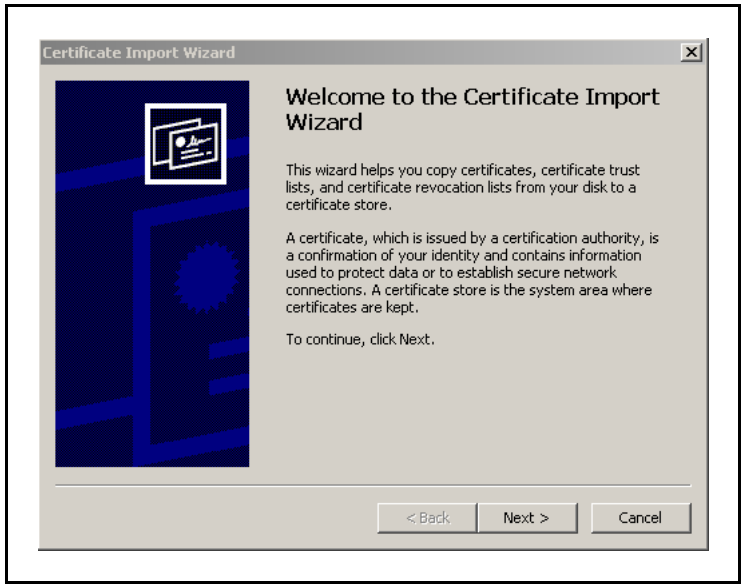


To copy the certificate information, click in the details window, press **ctrl-a** to select all of the text, and then press **ctrl-c** to copy the text.

4 Paste the copied text into a text editor, and save the file using the `.cer` file extension.

5 Right-click the `.cer` file, and select **Install certificate** from the shortcut menu.

The **Certificate Import Wizard** appears.



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

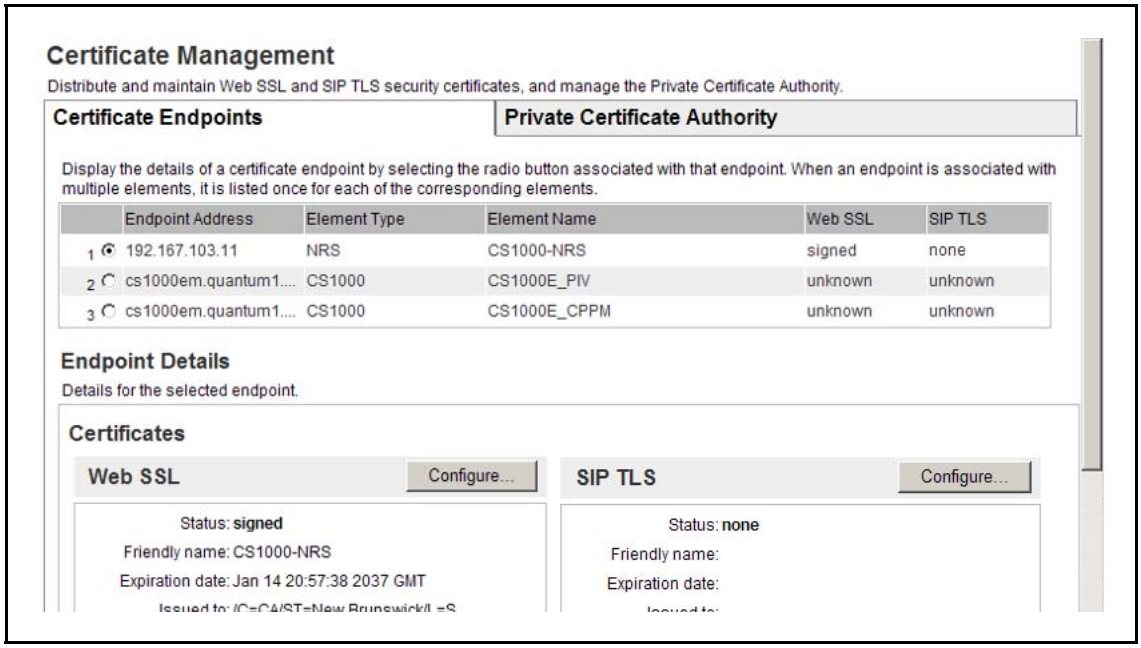
--End--

Add a CA to an endpoint

Use the following procedure to add a CA to a selected endpoint by using ECM.

Procedure 39
Adding a CA to an endpoint

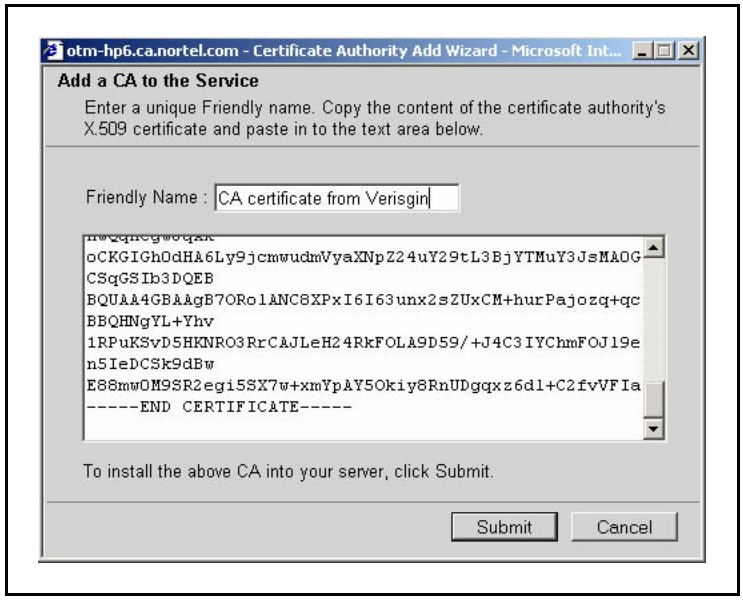
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



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

4 In the **Certificate Authorities** pane, click **Add**.

The **Add a CA to the Service** window appears.



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.

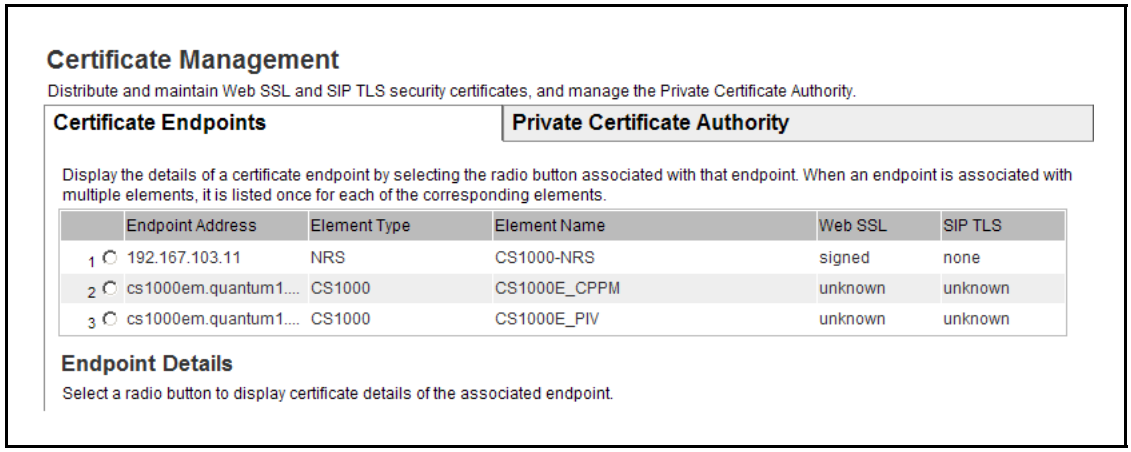
--End--

Change the trust status of an endpoint

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

Procedure 40
Changing the trust status of an endpoint certificate

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



3	In the **Certificate Endpoints** pane, select the option 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.

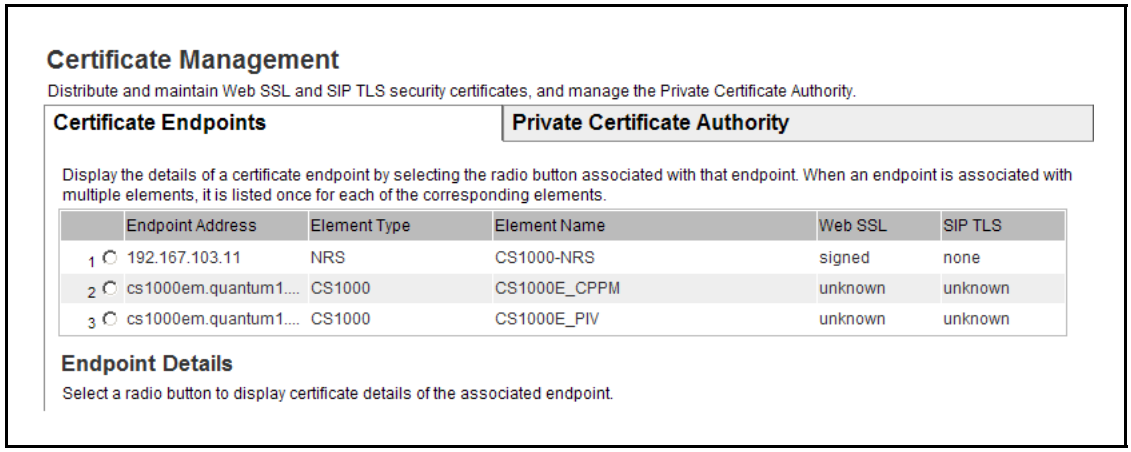
--End--

Delete a CA

Use the following procedure to delete a CA.

Procedure 41
Deleting a CA

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



3	In the **Certificate Endpoints** pane, select the option 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 ECM Certificate Management Wizard to complete the tasks listed in Table 38 "Certificate Management Wizard configuration options" (page 132).

Table 38
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 ECM to configure a certificate for an endpoint that is behind a firewall, open port 15080 to allow ECM to communicate with the endpoint, and 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 39 "Status types for certificate endpoints" (page 132).

Table 39
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 39
Status types for certificate endpoints (cont'd.)

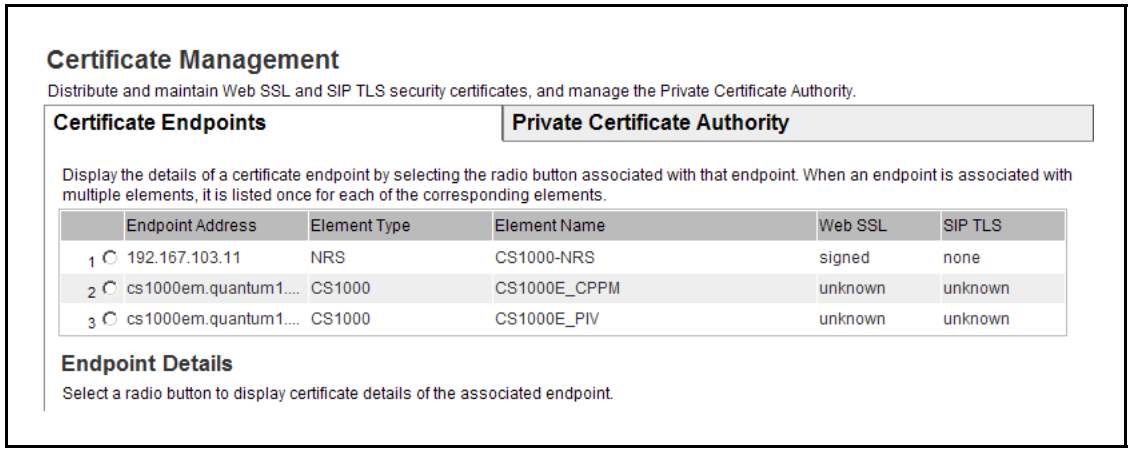
Status type	Description
about to expire	An X.509 certificate signed by a CA is issued for the service of the endpoint. The certificate will expire in less than 60 days.
expired	An X.509 certificate signed by a CA is issued for the service of the endpoint. The certificate has expired.

Certificate information

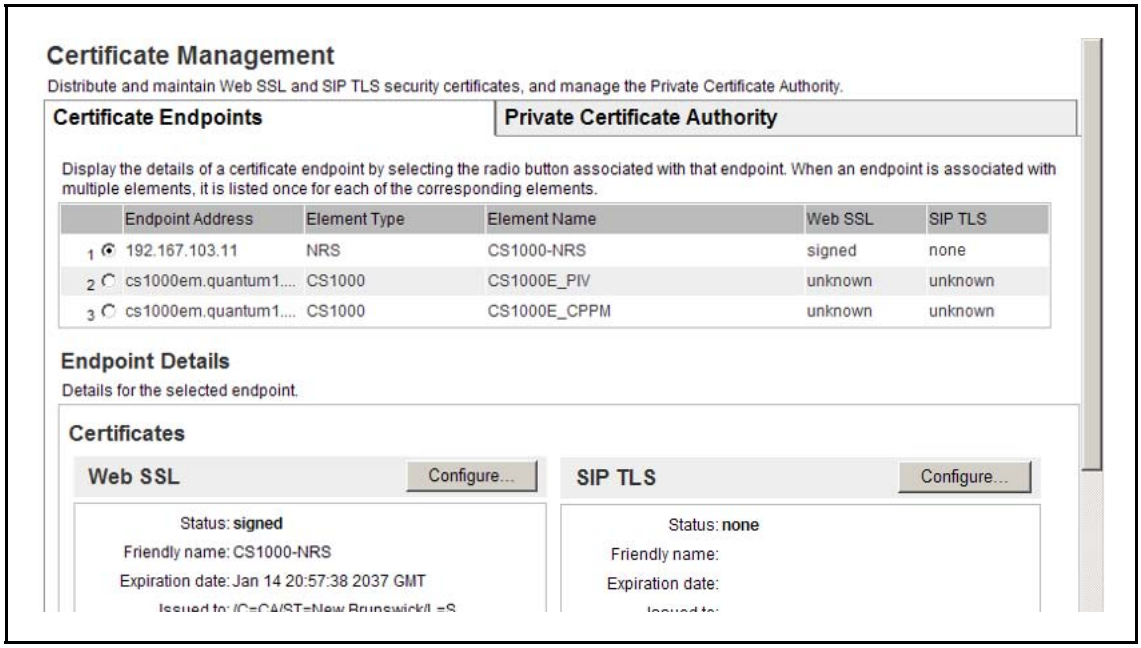
Use the following procedure to view the details about certificate endpoints and CAs.

Procedure 42
Viewing certificate details for an endpoint by using ECM

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



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears.



The status, and other information, for the selected endpoint is displayed in the Web SSL and SIP TLS pane. For more information about the different status types, see Table 39 "Status types for certificate endpoints" (page 132).

--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

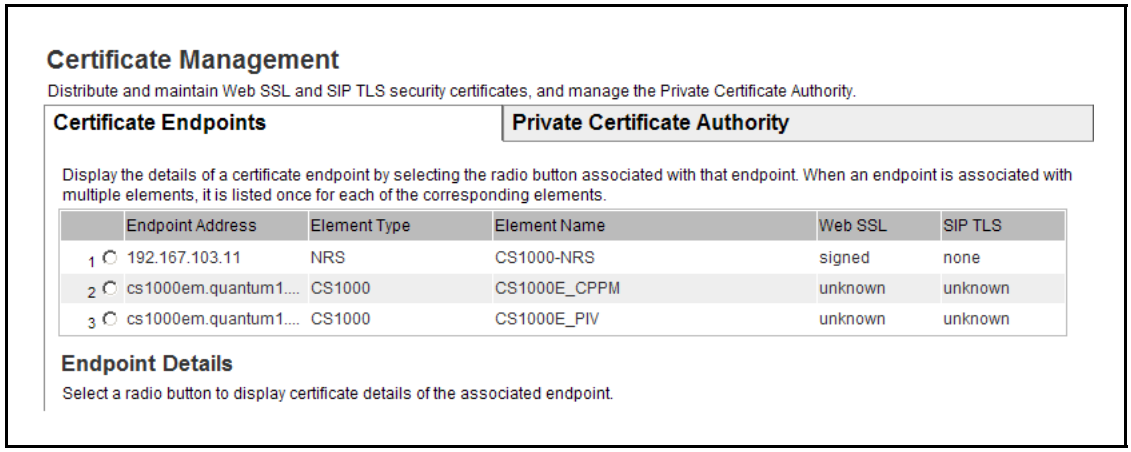
- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- Before you create a new certificate signed by a local private CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 43
Creating a certificate for Web SSL signed by the private CA

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

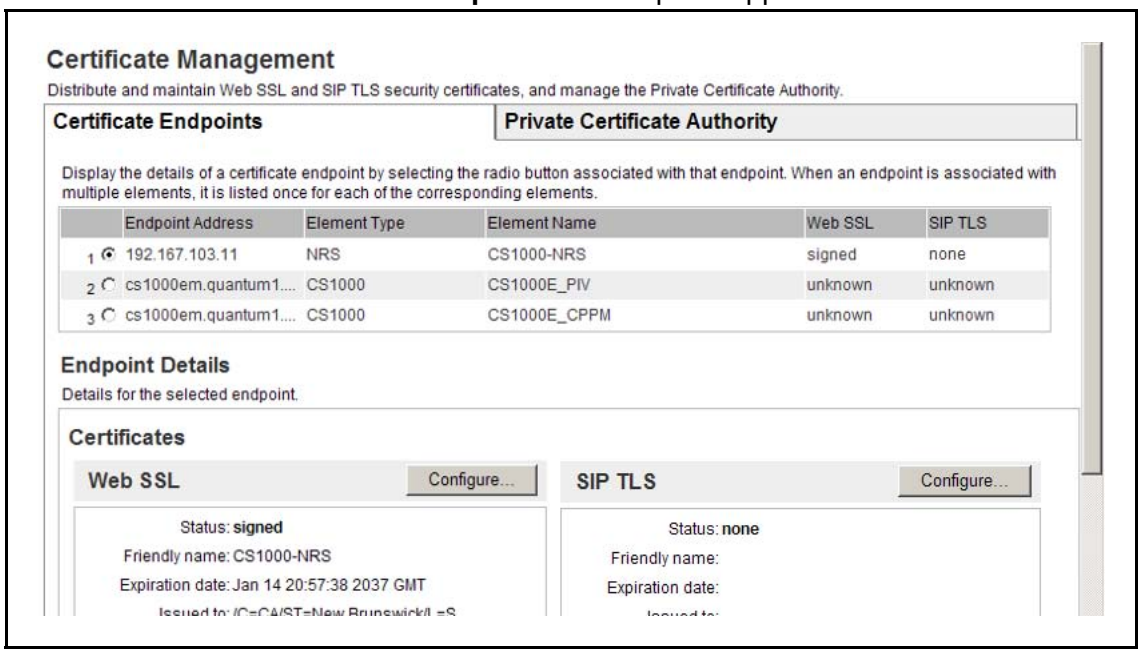
2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



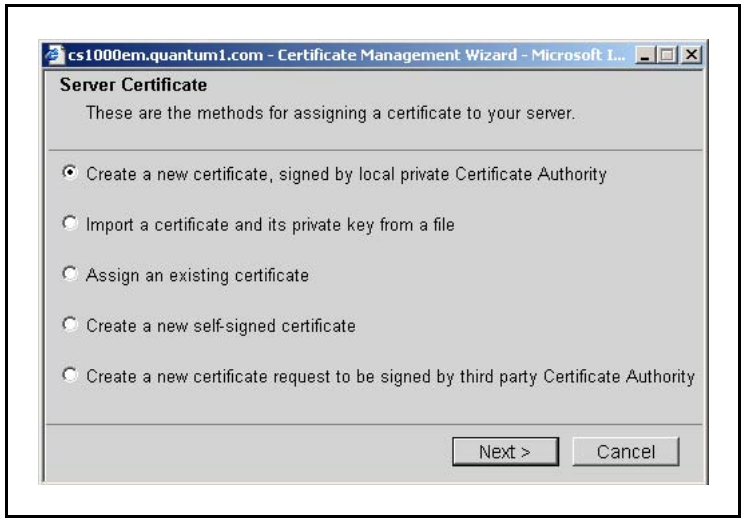
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** pane appears.



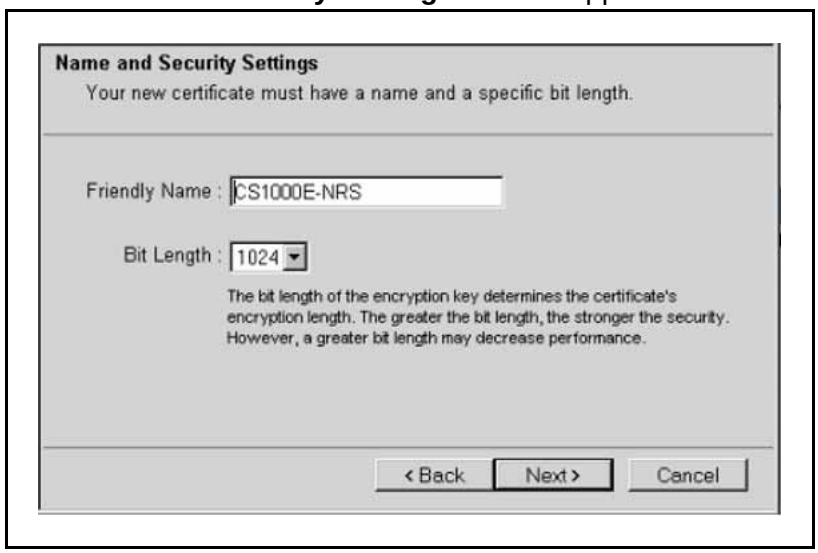
4 In the **Web SSL** pane, click **Configure**.

The **Server Certificate** window appears.



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

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

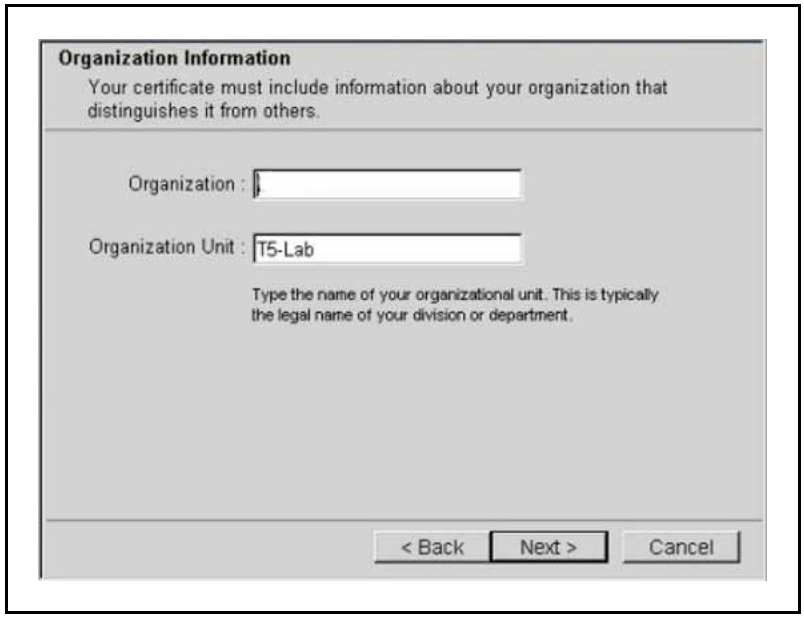


6 Type a name in the **Friendly Name** field.

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

8 Click **Next**.

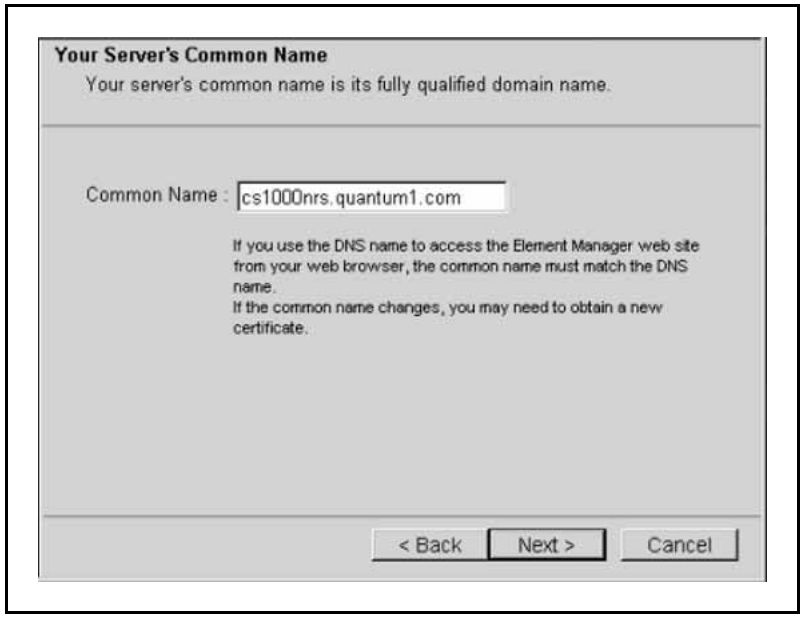
The **Organization Information** window appears.



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

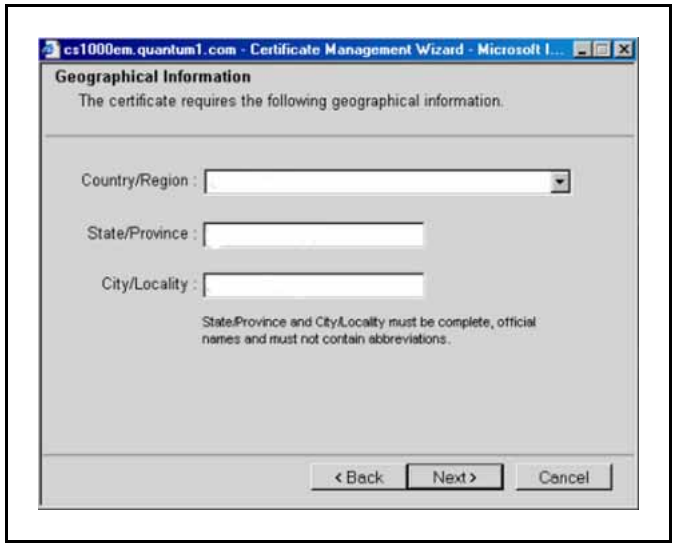
- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

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



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

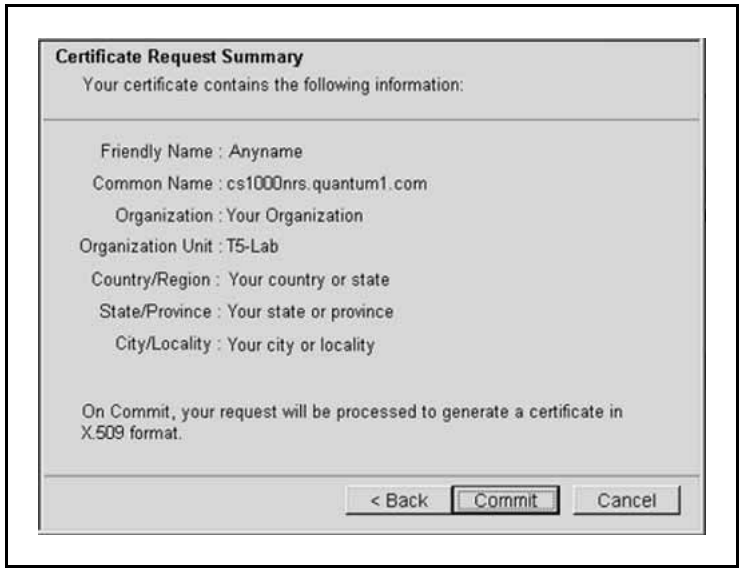
The **Geographical Information** window appears.



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

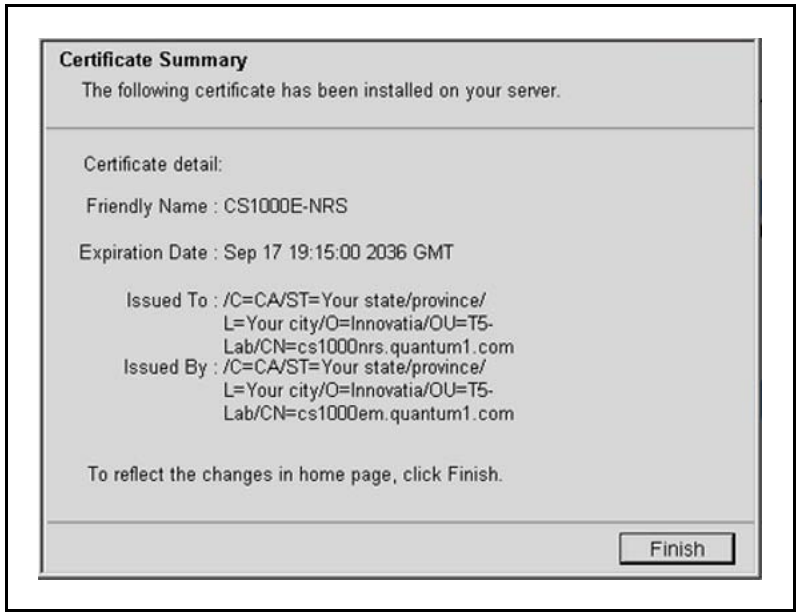
- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



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

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



13 Click **Finish**.

The status changes to signed.

14 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

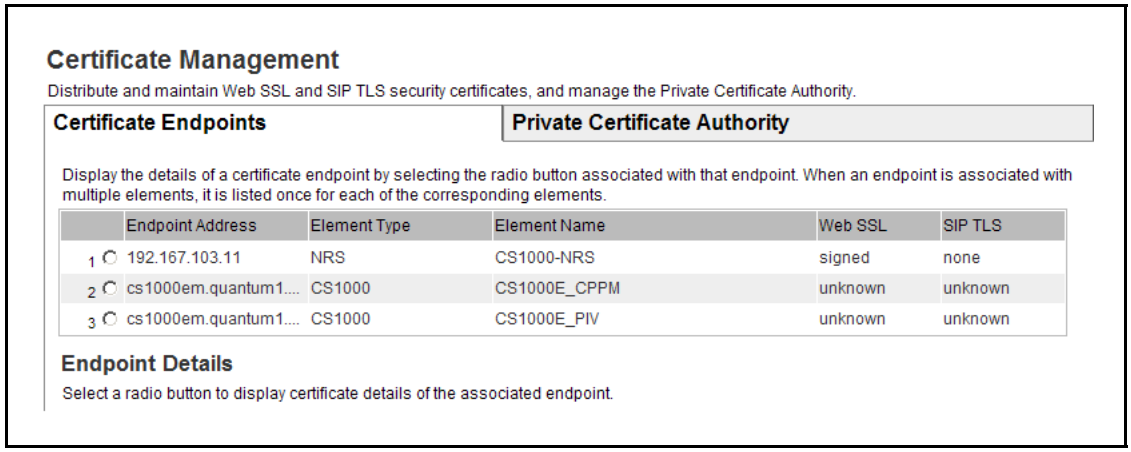
- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- Before you create a request 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 39 "Status types for certificate endpoints" (page 132).

Procedure 44
Creating a request for a certificate for Web SSL signed by third-party CA

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

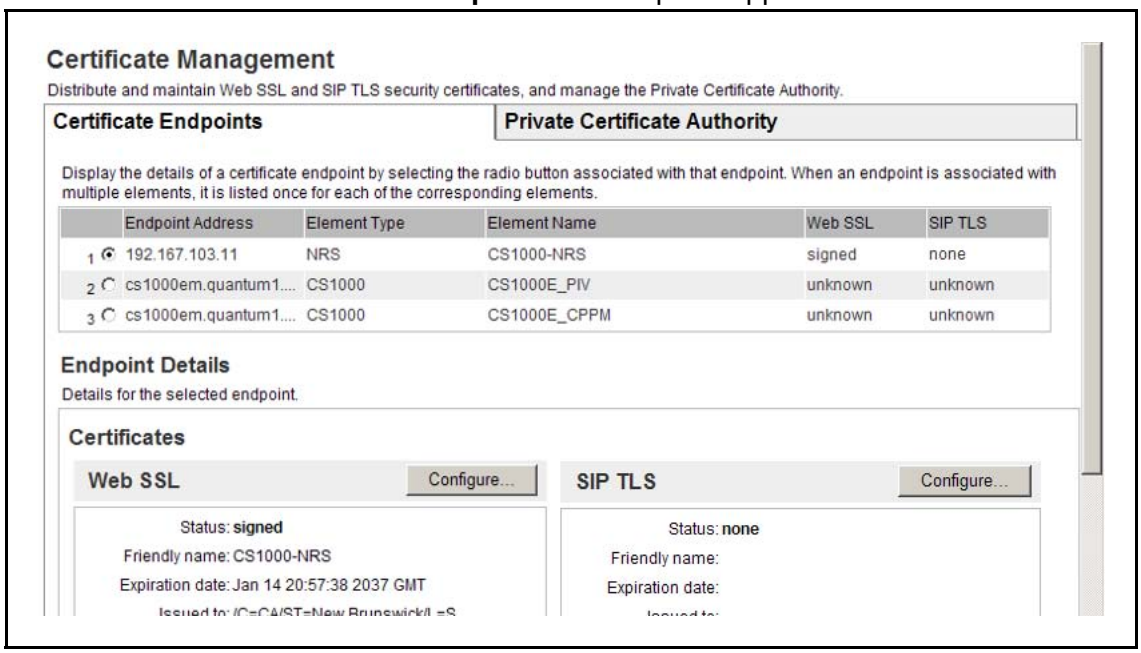
2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



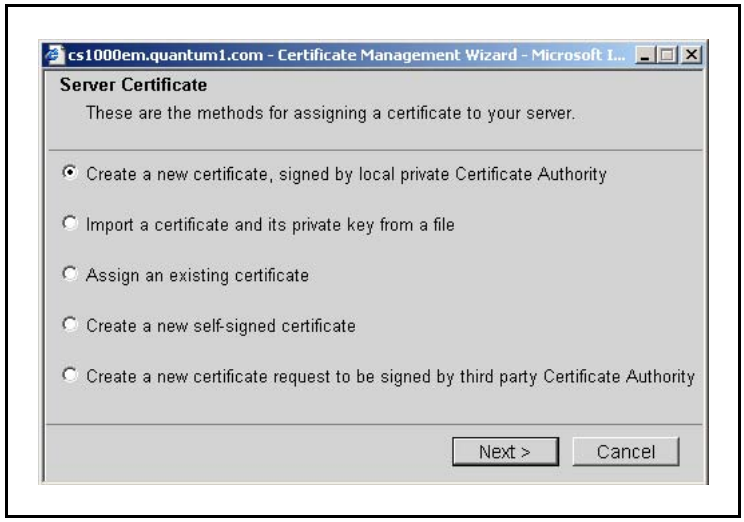
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** pane appears.



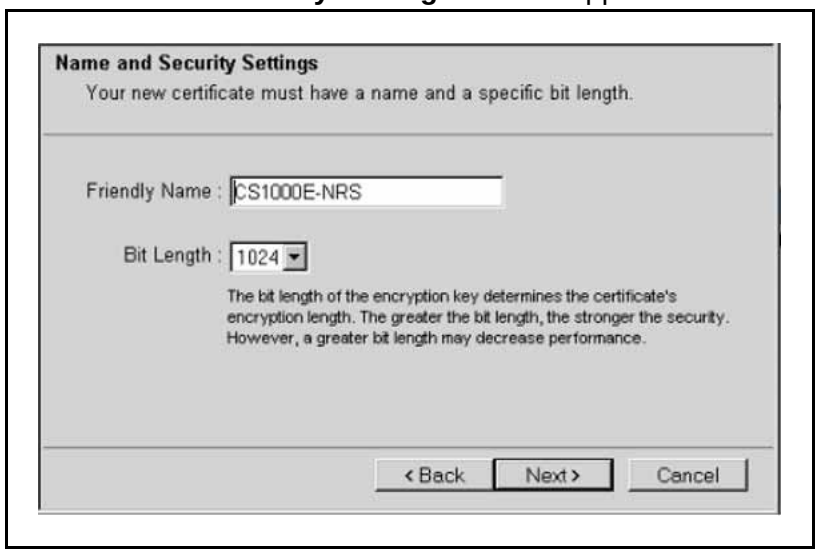
4 In the **Web SSL** section of the **Certificates** pane, click **Configure**.

The **Server Certificate** window appears.



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

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

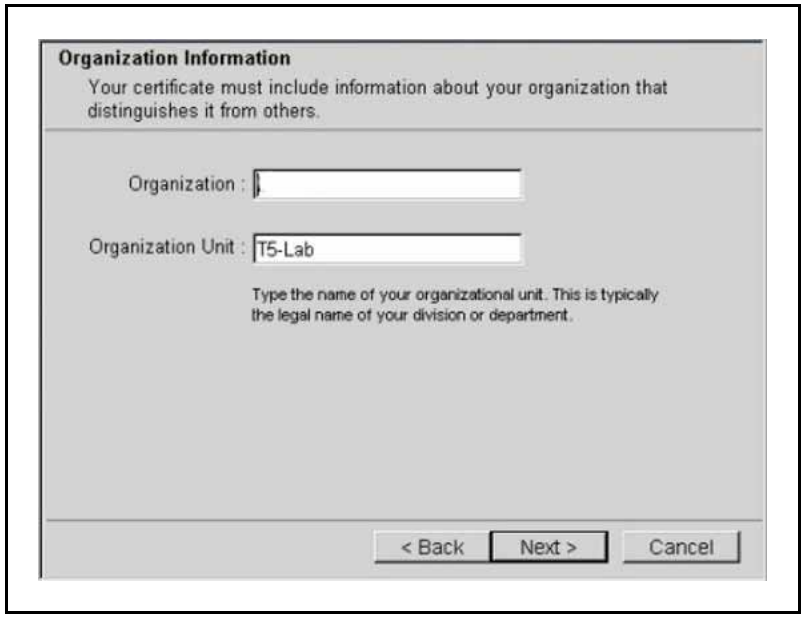


6 Type a name in the **Friendly Name** field.

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

8 Click **Next**.

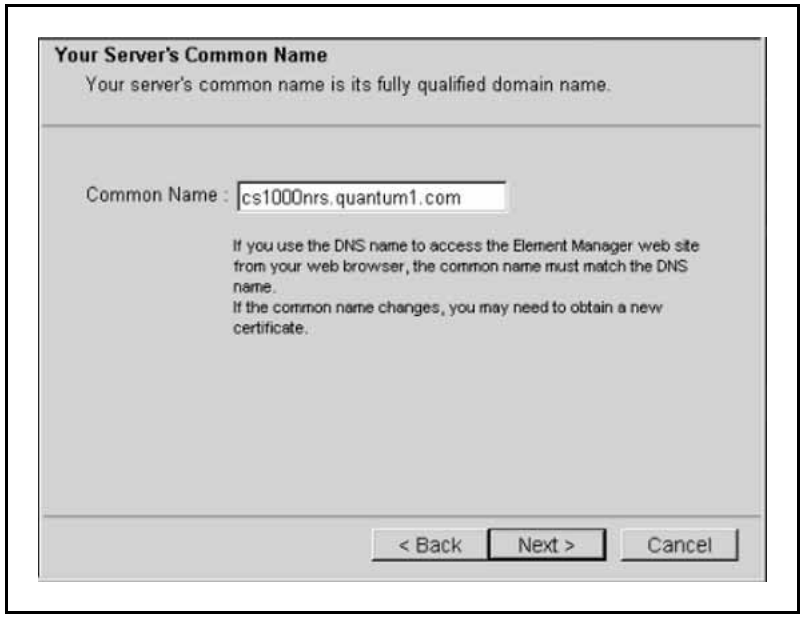
The **Organization Information** window appears.



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.



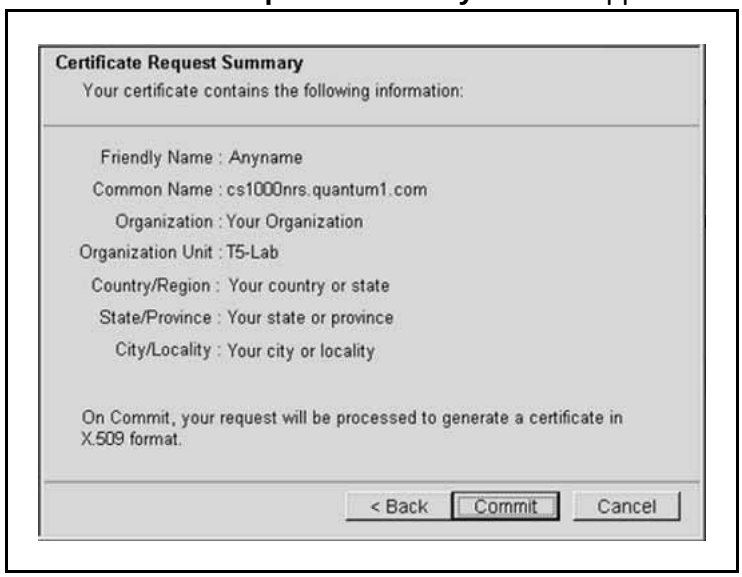
10 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.

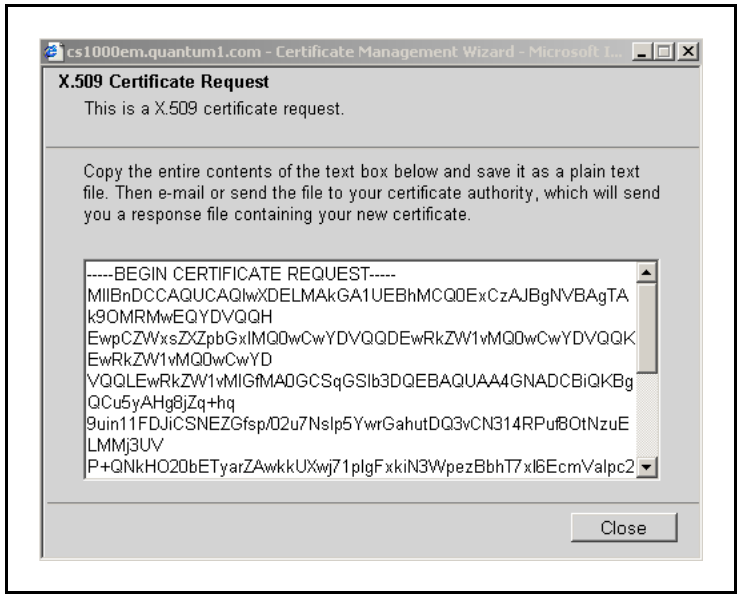
11 In the **Geographical Information** , perform the following tasks:

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

The **Certificate Request Summary** window appears.



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



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 51 “Processing a pending certificate request by using ECM” (page 171).

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 39 “Adding a CA to an endpoint” (page 128) to add the intermediate CA to the browser.

Create a self-signed certificate for Web SSL

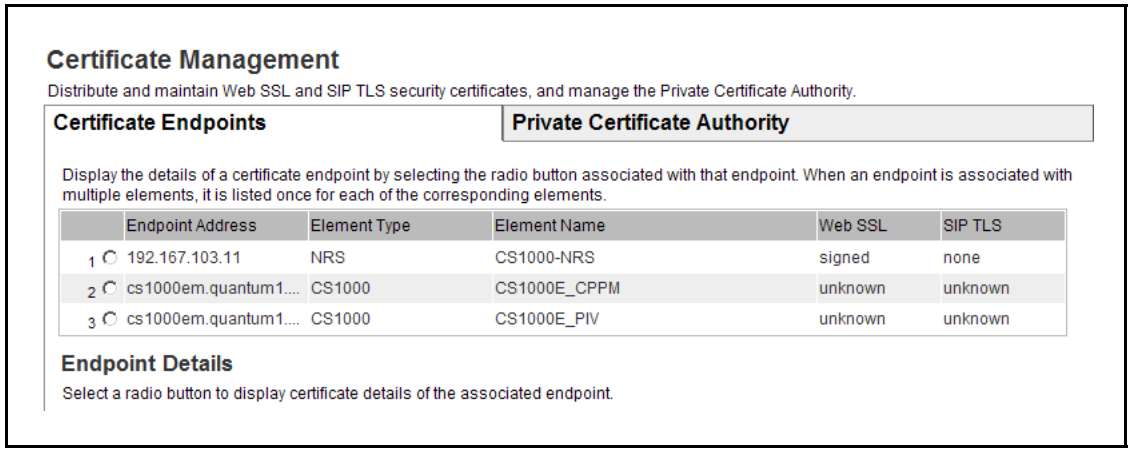
Use the following procedure to create a new self-signed certificate.

Prerequisites

- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- 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 39 "Status types for certificate endpoints" (page 132).

Procedure 45
Creating a self-signed certificate for Web SSL

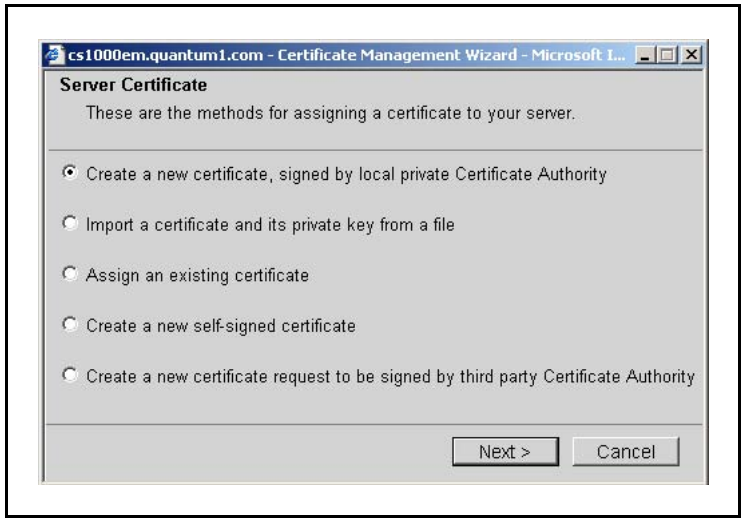
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none. The **Endpoint Details** pane appears.

4	On the **Certificate Management** page, in the **Web SSL** pane, click **Configure**.

The **Server Certificate** window appears.



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

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

6 Click **Next**.

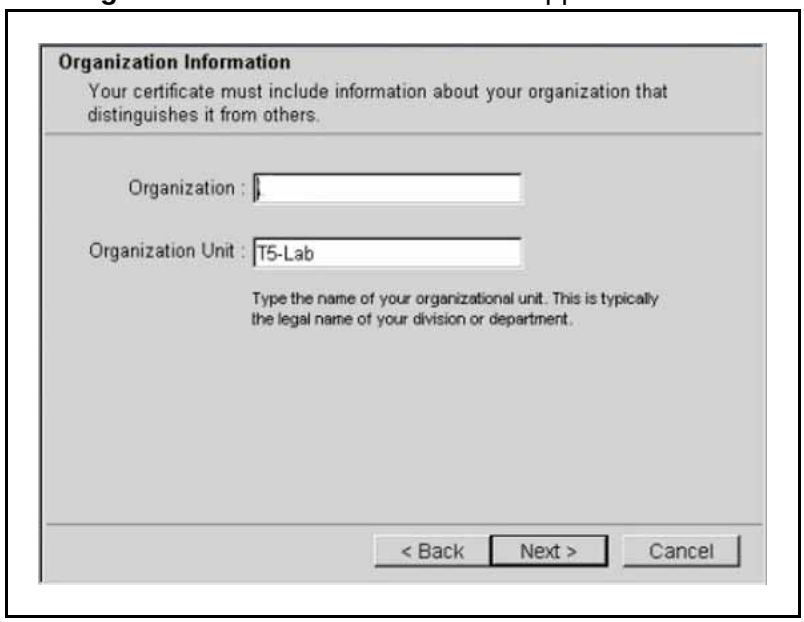
The **Name and Security Settings** window appears.

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

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

9 Click **Next**.

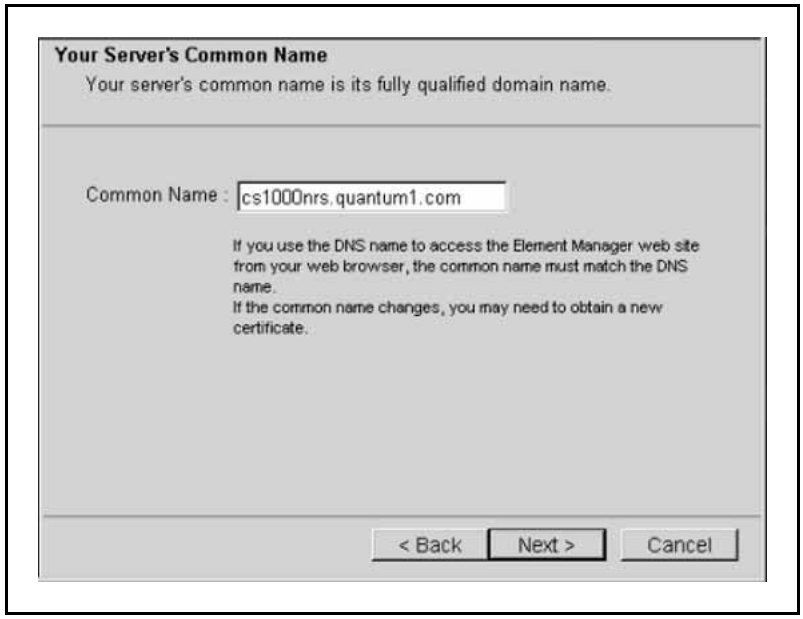
The **Organization Information** window appears.



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

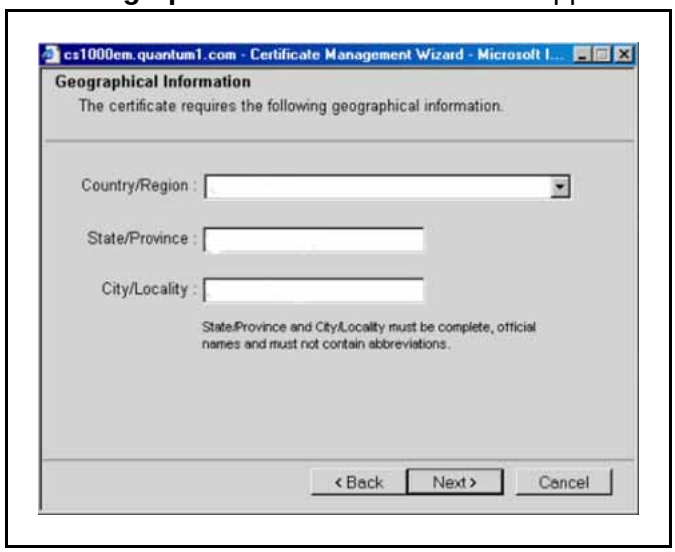
- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

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



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

The **Geographical Information** window appears.



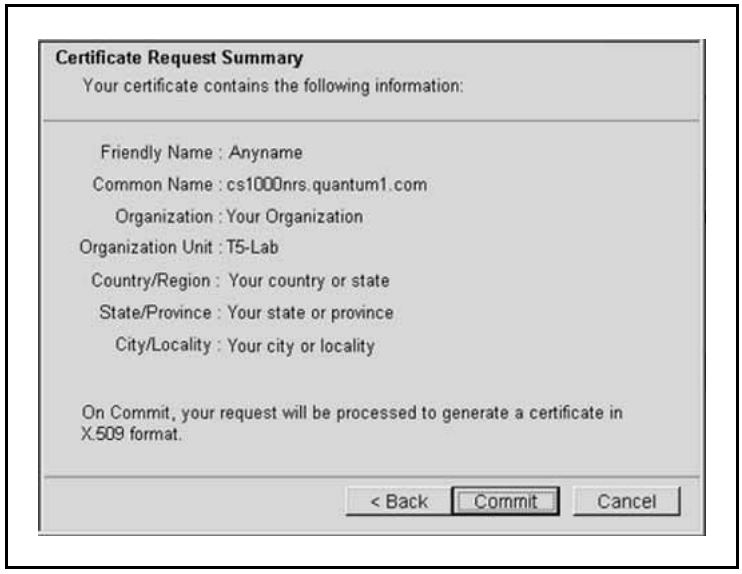
12 Enter a **Country/Region**.

13 Enter a **State/Province**.

14 Enter a **City/Locality**.

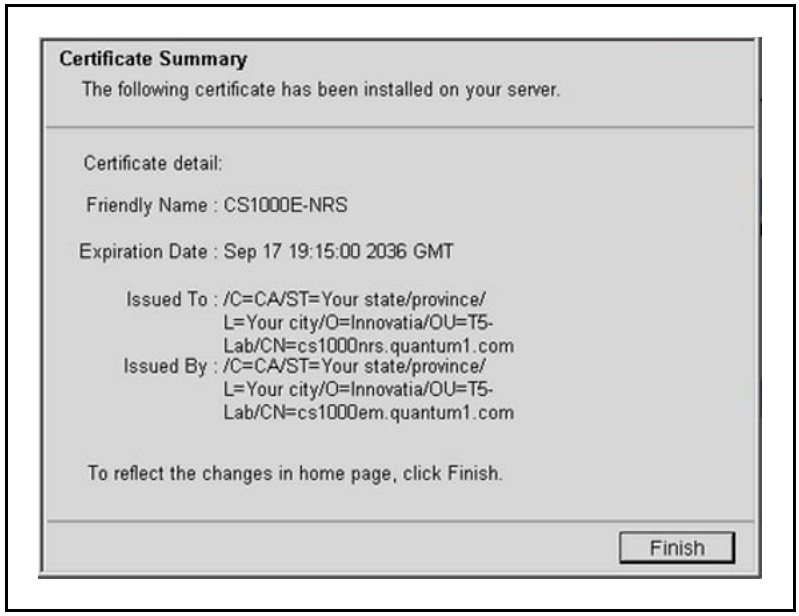
15 Click **Next**.

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.

--End--

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

- Follow the steps in Procedure 54 “Exporting the current self-signed certificate by using ECM” (page 178) to export the self-signed certificate.
- Follow the steps in Procedure 39 “Adding a CA to an endpoint” (page 128) 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

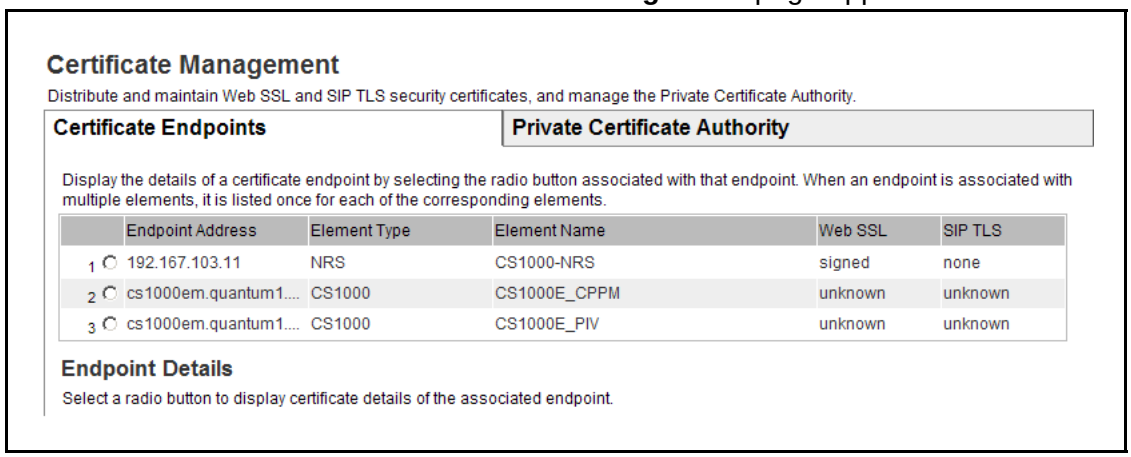
Use the following procedure to create a new certificate request that is signed by a private CA.

Prerequisites

- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- 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 39 "Status types for certificate endpoints" (page 132).

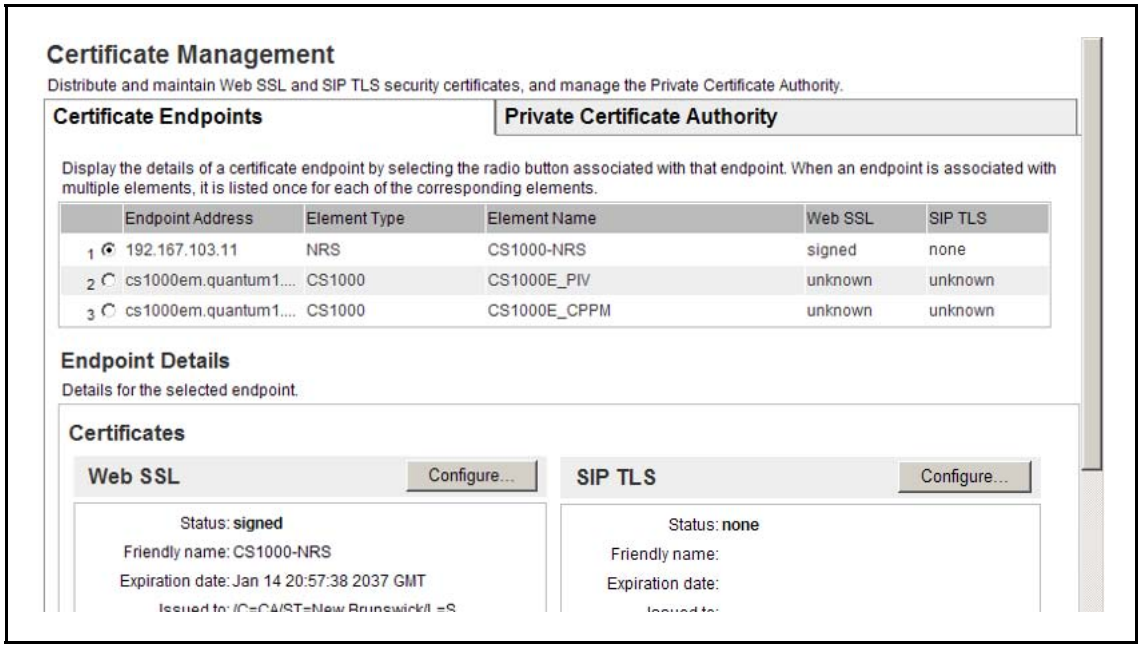
Procedure 46
Creating a certificate for SIP TLS signed by the private CA

Step	Action
1	Click **Security** > **Certificates**. The **Certificate Management** page appears.



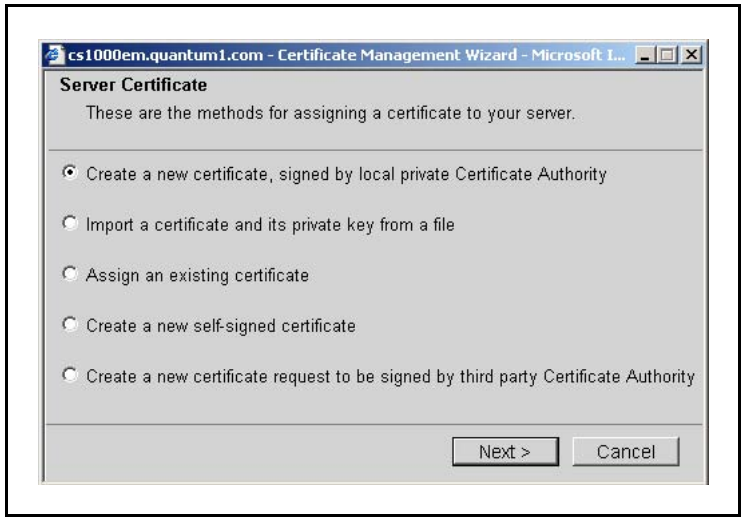
2	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** pane appears.

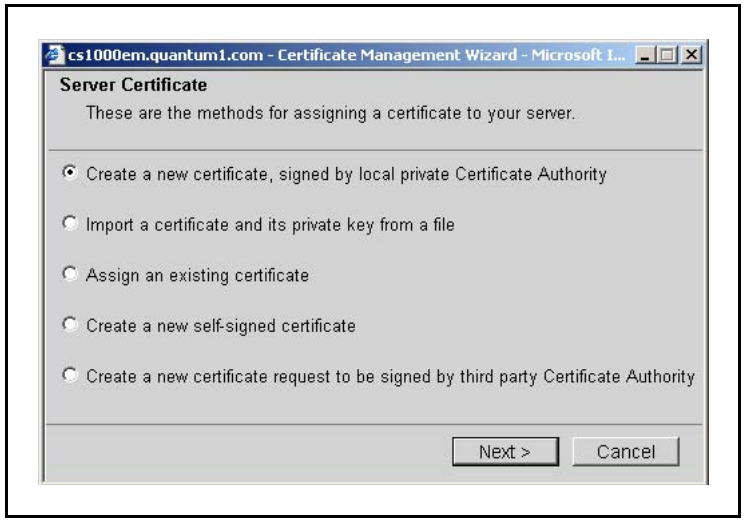


3 In the **SIP TLS** pane, click **Configure**.

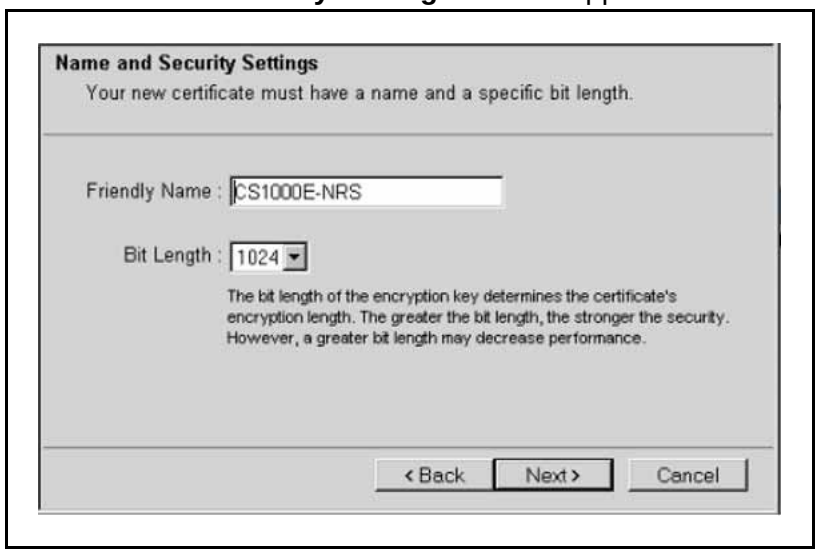
The **Server Certificate** window appears.



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



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

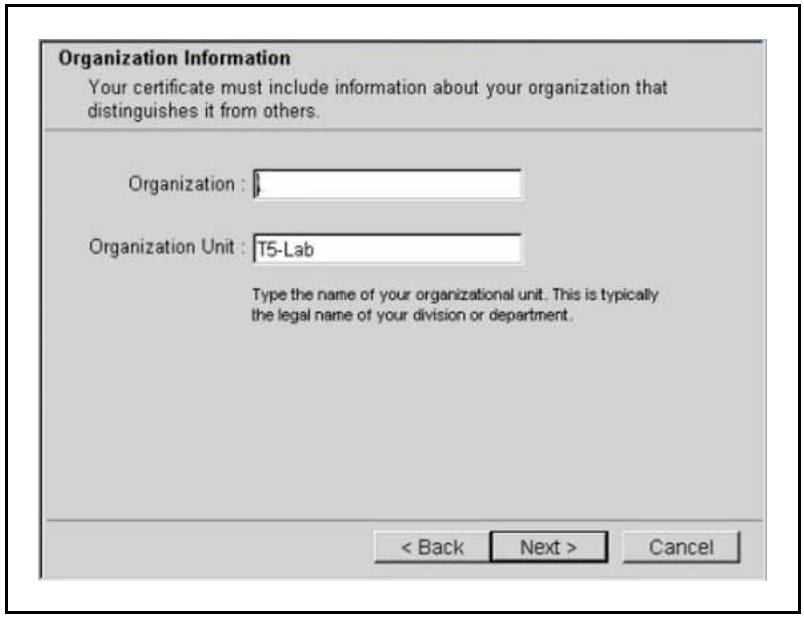


5 Type a name in the **Friendly Name** field.

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

7 Click **Next**.

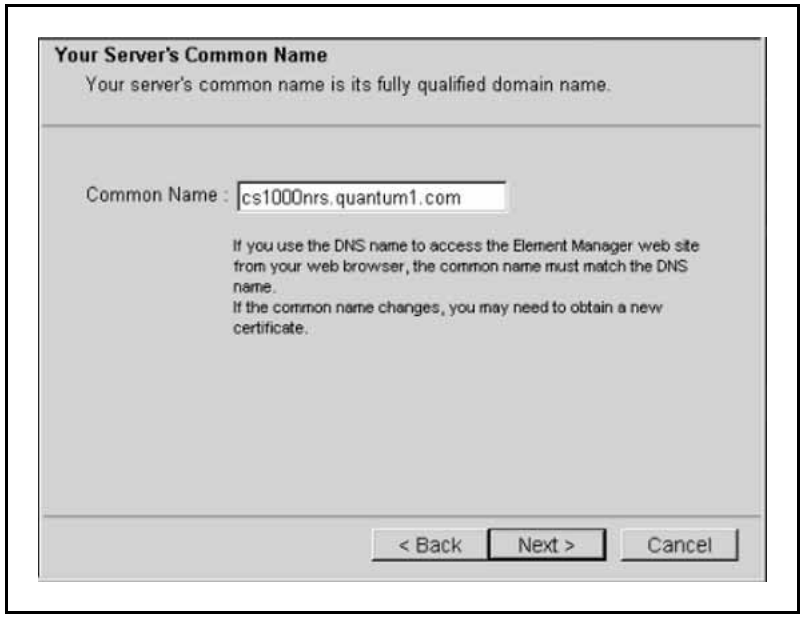
The **Organization Information** window appears.



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

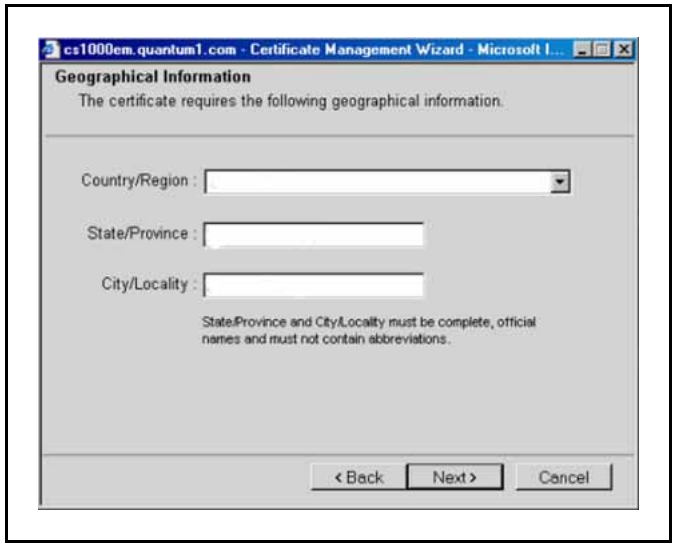
- In the **Organization** field, enter the Organization.
- In the **Organization Unit** field, enter the organization unit information.
- Click **Next**.

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



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

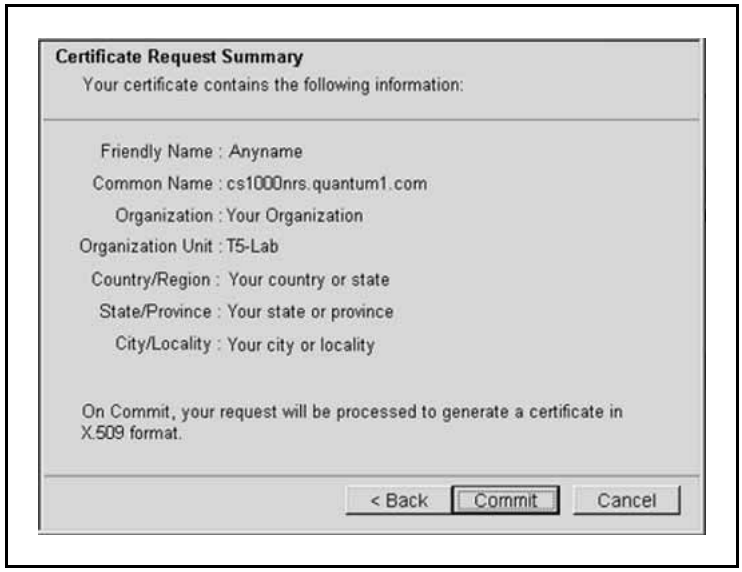
The **Geographical Information** window appears.



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

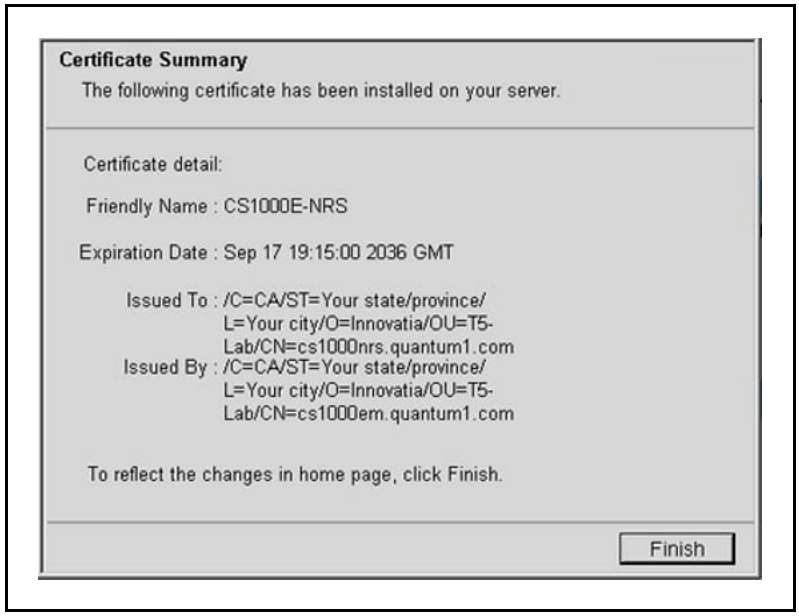
- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



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

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



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 CS 1000 Release 4.5 to CS 1000 Release 5.5, see “Create a request for a third-party CA certificate for SIP TLS when upgrading the system” (page 160) before you proceed.

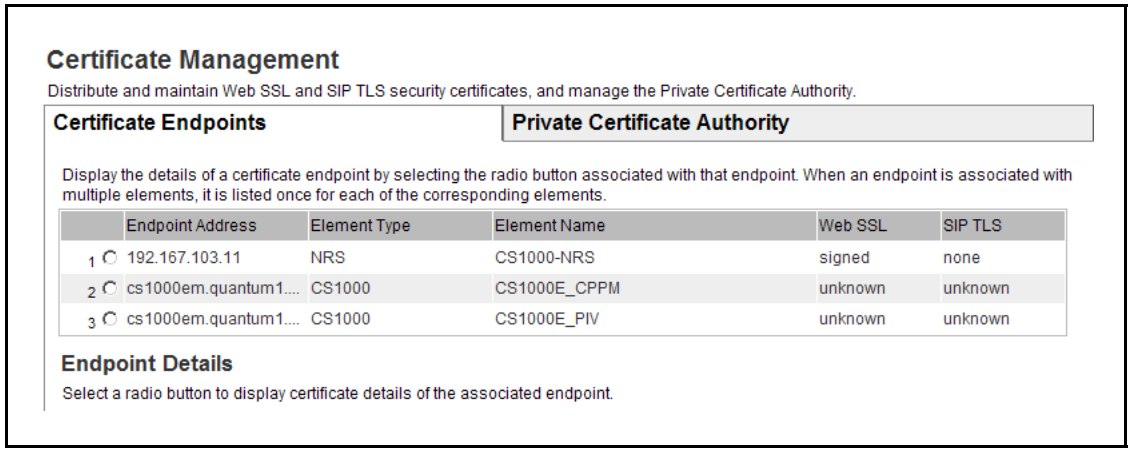
Use the following procedure to create a certificate request to be signed by a third-party CA for a SIP Proxy or new SIP Gateway system.

Prerequisites

- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- 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 39 "Status types for certificate endpoints" (page 132).

Procedure 47
Creating a request for a certificate for SIP TLS signed by a public CA

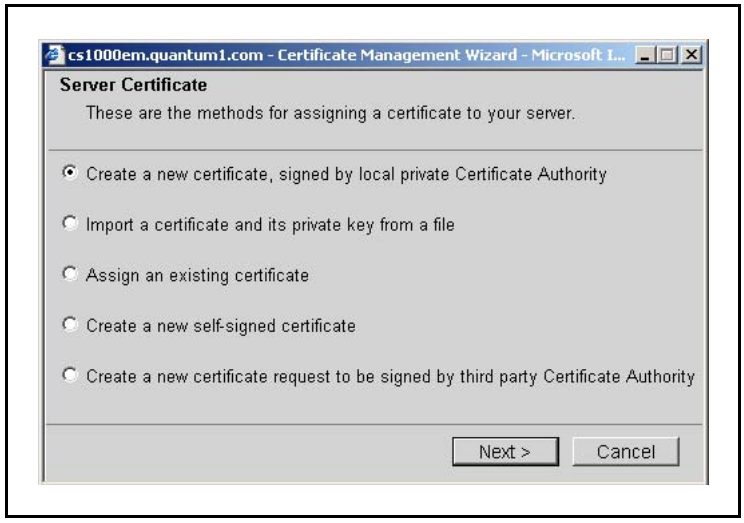
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none. The **Endpoint Details** pane appears.

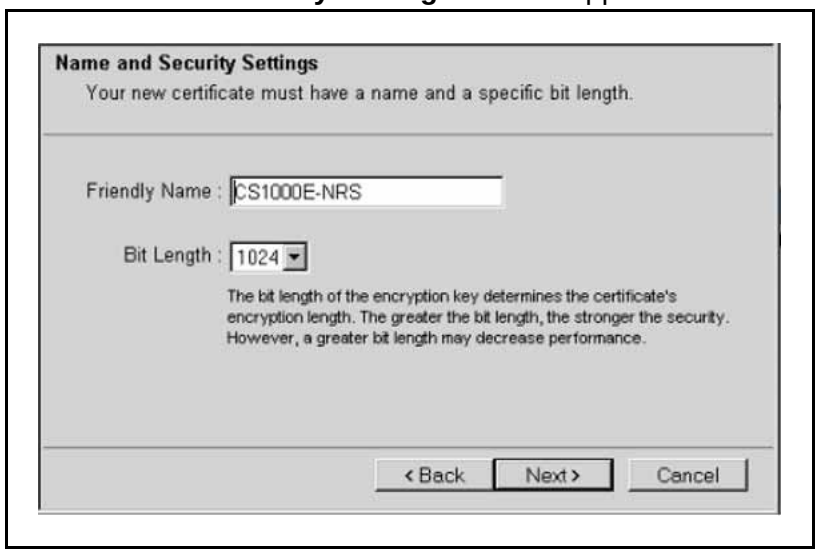
4	In the **SIP TLS** pane, click **Configure**.

The **Server Certificate** window appears.



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

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

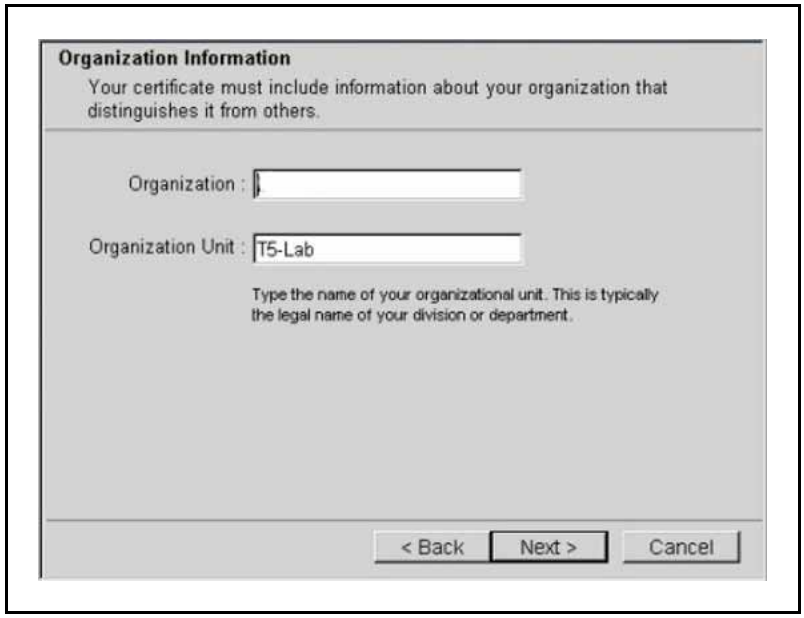


6 Type a name in the **Friendly Name** field.

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

8 Click **Next**.

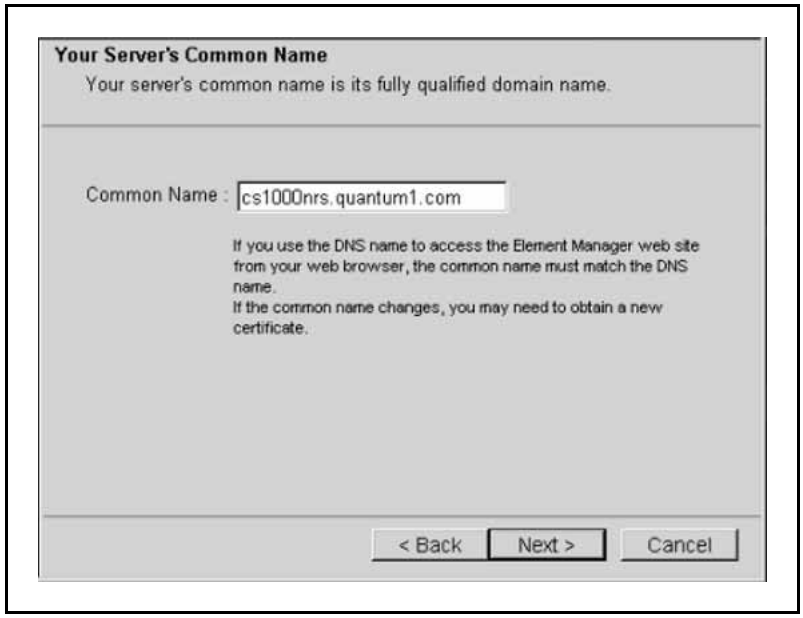
The **Organization Information** window appears.



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.



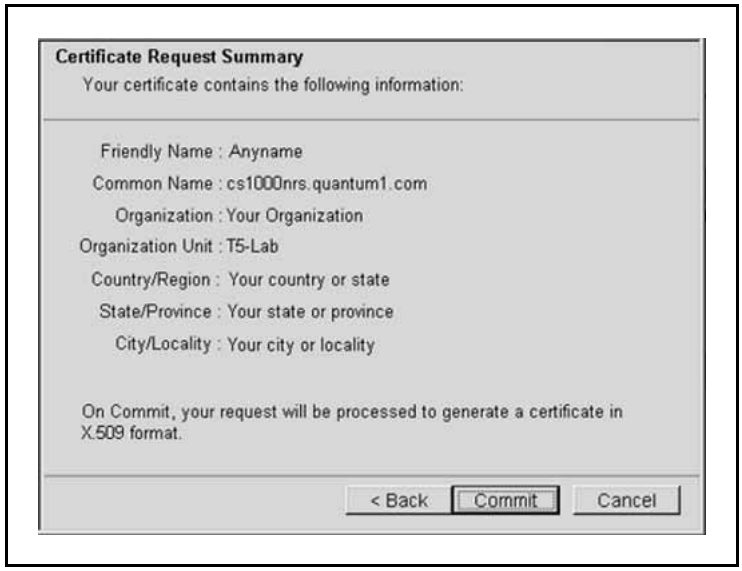
10 Enter the FQDN of the server you are configuring in the **Common Name** field, and click **Next**.

The **Geographical Information** window appears.

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

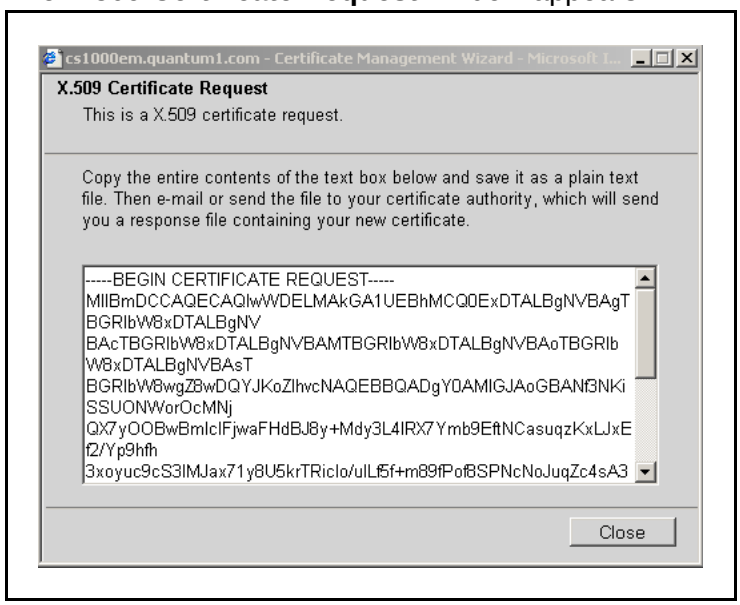
- In the **Country/Region** box, select the country from the list.
- In the **State/Province** field, enter the state or province.
- In the **City/Locality** field, enter the city or locality.
- Click **Next**.

The **Certificate Request Summary** window appears.



12 Click **Commit**.

The **X.509 Certificate Request** window appears.



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 51 “Processing a pending certificate request by using ECM” (page 171).

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 39 “Adding a CA to an endpoint” (page 128) to add the intermediate CA to the server.

For more information about certificate chains, see Table 11 "Examples of certificates in a chain" (page 38).

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 CS 1000 Release 4.5 to CS 1000 Release 5.5, 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.

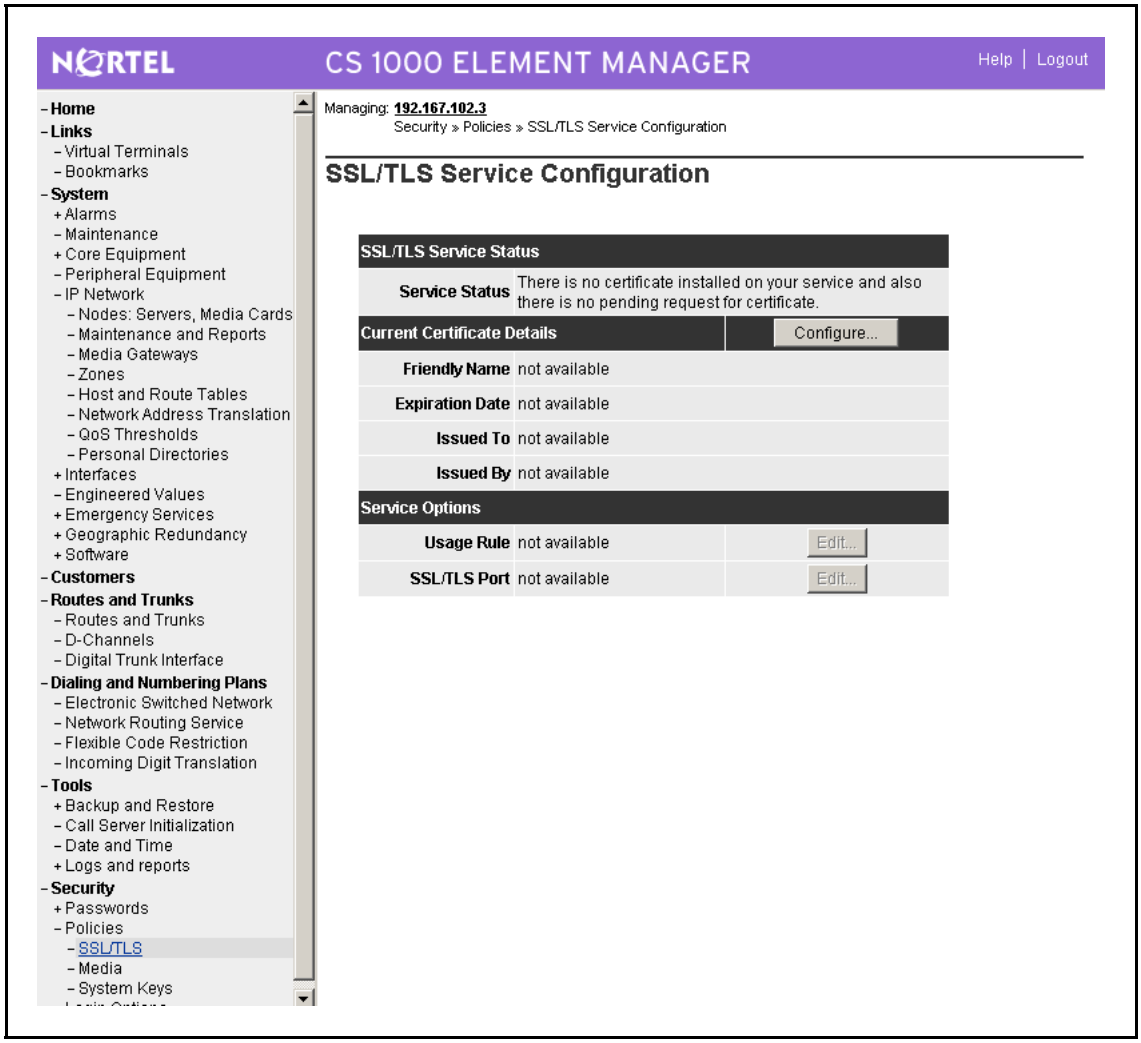
If you have already upgraded the system from CS 1000 Release 4.5 to CS 1000 Release 5.5, see Procedure 47 “Creating a request for a certificate for SIP TLS signed by a public CA ” (page 156). If you have not yet upgraded the system see Procedure 48 “Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading” (page 161) 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 48
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 4.5, log on to Element Manager using a System password level 2 account.
2	Click **Security** > **SSL/TLS**. The **SSL/TLS Service Configuration** page appears.



3 Click **Configure**.

The **Server Certificate** window appears.

4 Select **Create a new certificate request to be signed by Certificate Authority**.

5 Click **Next**.

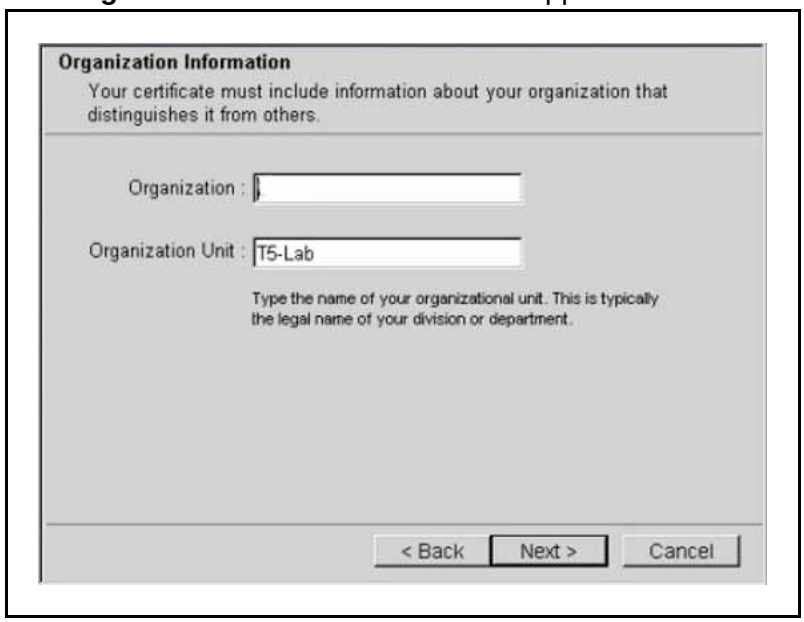
The **Name and Security Settings** window appears.

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

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

8 Click **Next**.

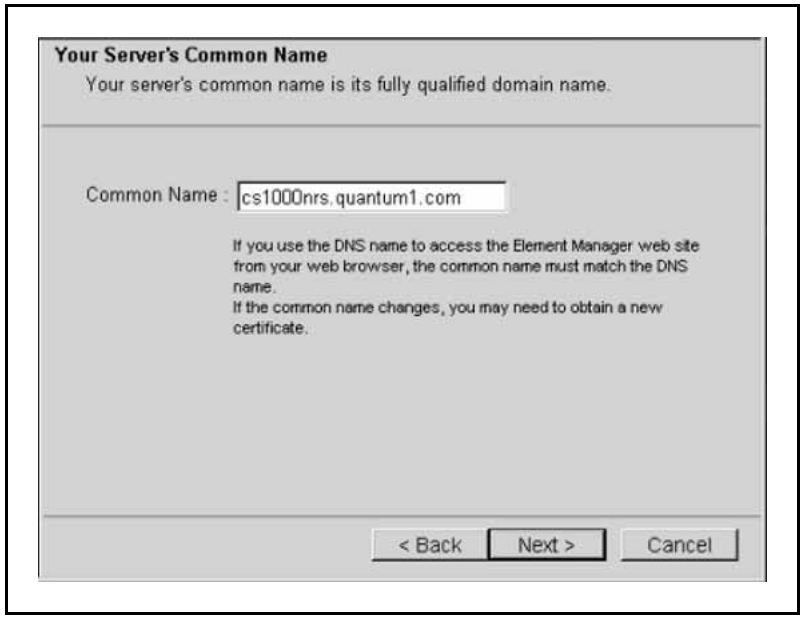
The **Organization Information** window appears.



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.



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.

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.

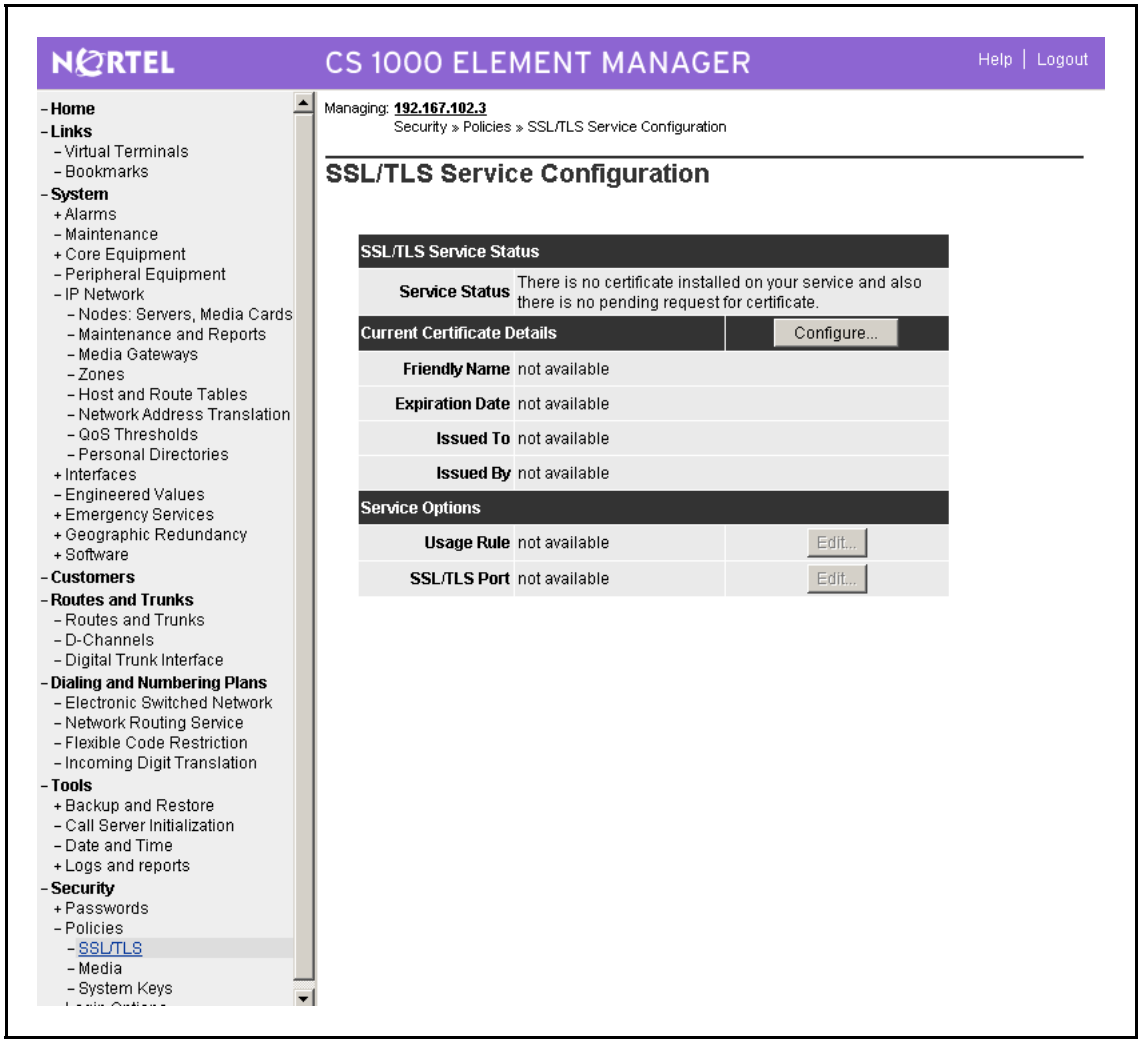
--End--

Use the following procedure to process a pending certificate response using Element Manager. If you have already upgraded the system from CS 1000 Release 4.5 to CS 1000 Release 5.5, see Procedure 47 “Creating a request for a certificate for SIP TLS signed by a public CA ” (page 156)

- 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 49
Processing a pending certificate response for SIP TLS when upgrading

Step	Action
1	Before upgrading from CS 1000 Release 4.5, log on to Element Manager using a System password level 2 account.
2	Click **Security** > **SSL/TLS**. The **SSL/TLS Service Configuration** page appears.



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 5.5.

8 Follow the steps in Adding a CS 1000 Release 5.0 system to the list of ECM managed elements to add an element.

9 Follow the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57) to add an element.

10 Follow the steps in Procedure 57 “Assigning an existing certificate by using ECM” (page 186) to assign the installed third-party CA certificate.

11 Use the steps in Procedure 39 “Adding a CA to an endpoint” (page 128) 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

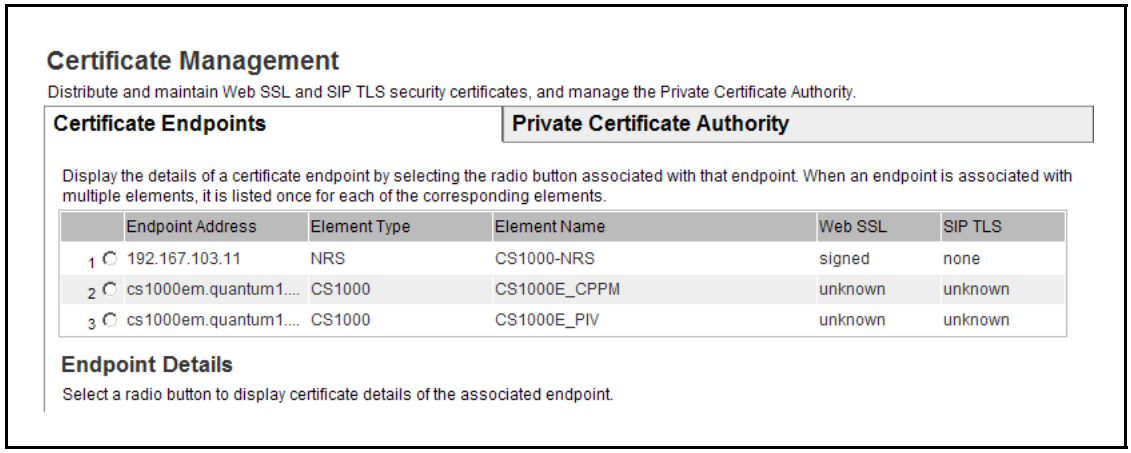
Use the following procedure to create a new self-signed certificate.

Prerequisites

- Certificates are added to ECM network elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).
- 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 39 "Status types for certificate endpoints" (page 132).

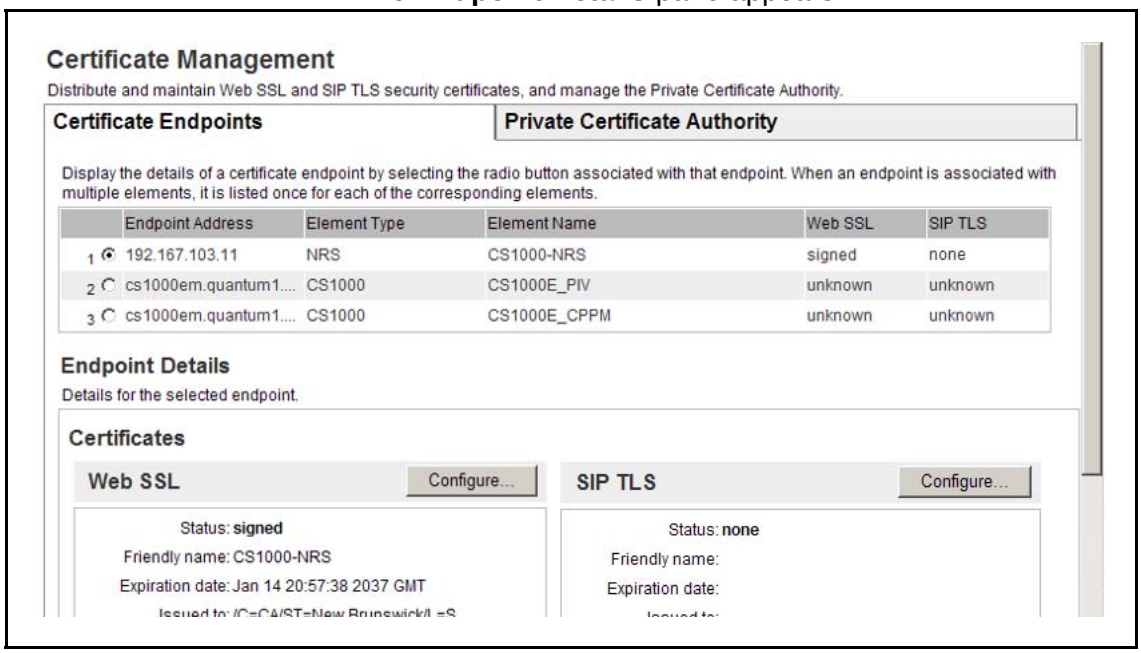
Procedure 50
Creating a self-signed certificate for SIP TLS

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



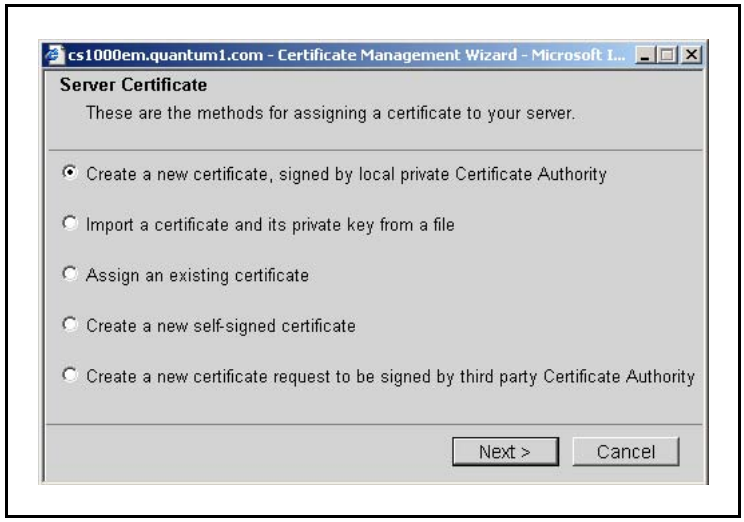
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure; the certificate endpoint status must be none.

The **Endpoint Details** pane appears.



4 In the **SIP TLS** pane, click **Configure**.

The **Server Certificate** window appears.

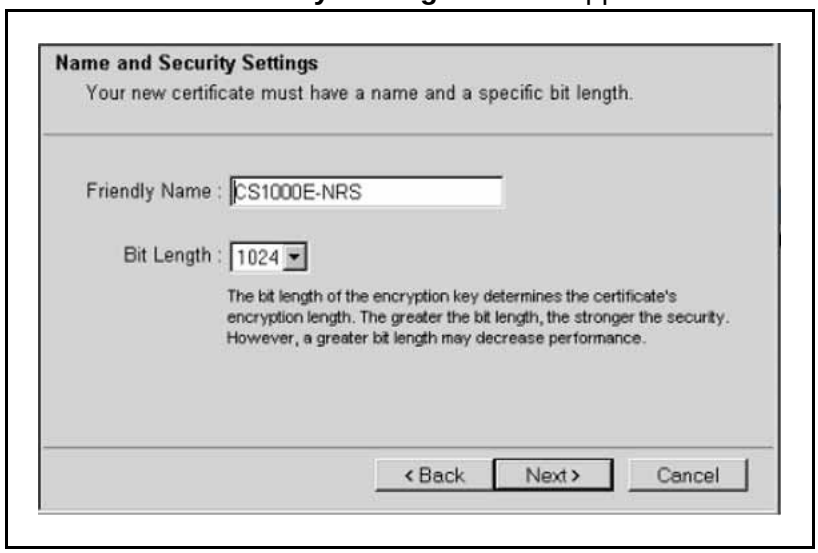


5 Select **Create a new self-signed certificate**, and click **Next**.

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

6 Click **Next**.

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

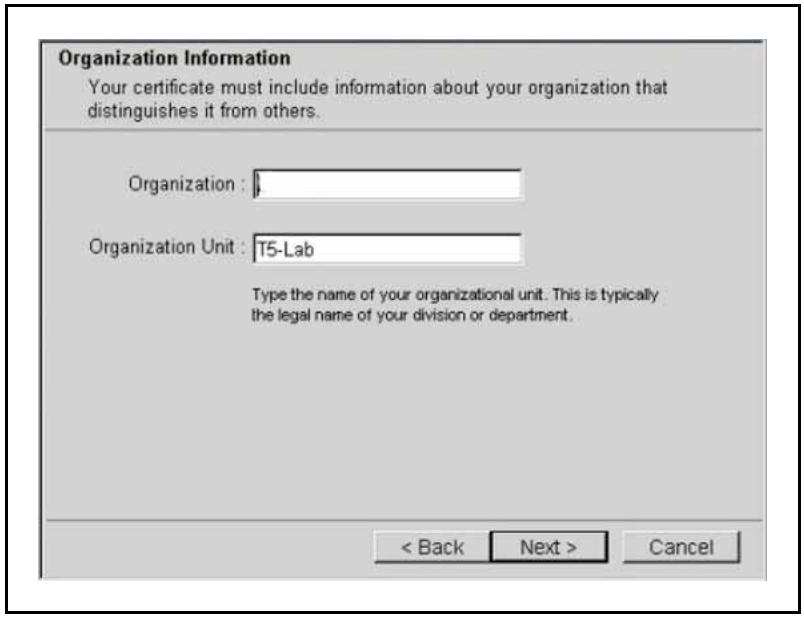


7 Type a name in the **Friendly Name** field.

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

9 Click **Next**.

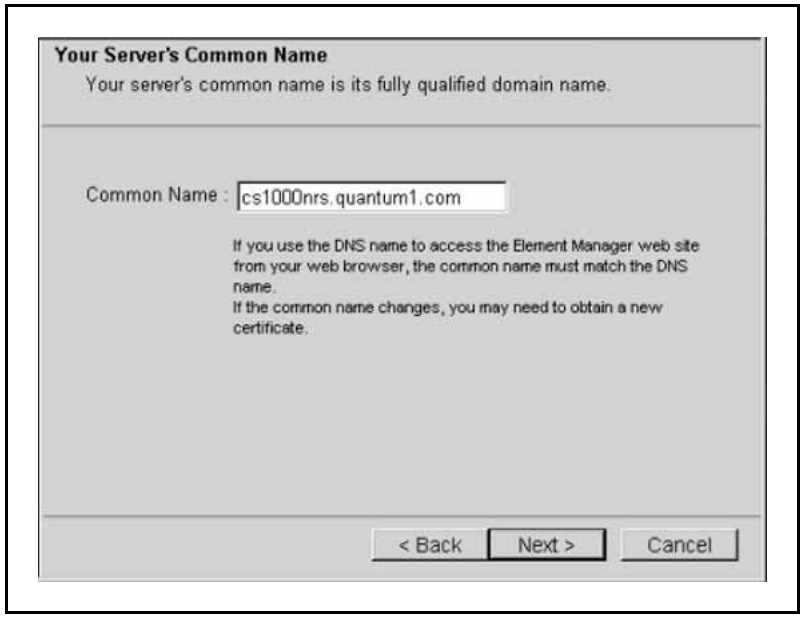
The **Organization Information** window appears.



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.



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 54 “Exporting the current self-signed certificate by using ECM” (page 178) to export the self-signed certificate.

20 Use the steps in Procedure 39 “Adding a CA to an endpoint” (page 128) 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 155). 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

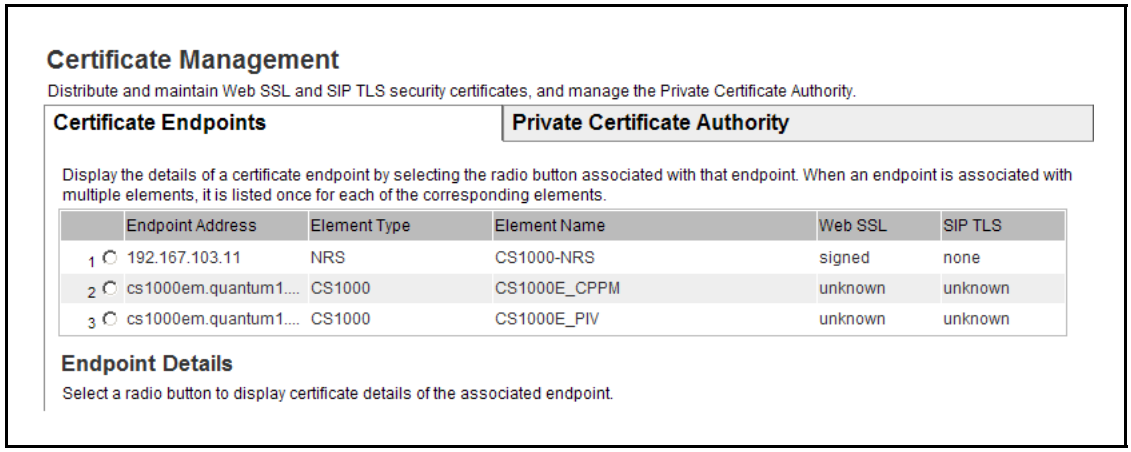
- Before you process a pending certificate request, ensure that the certificate endpoint status is pending or pending renew. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 51
Processing a pending certificate request by using ECM

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

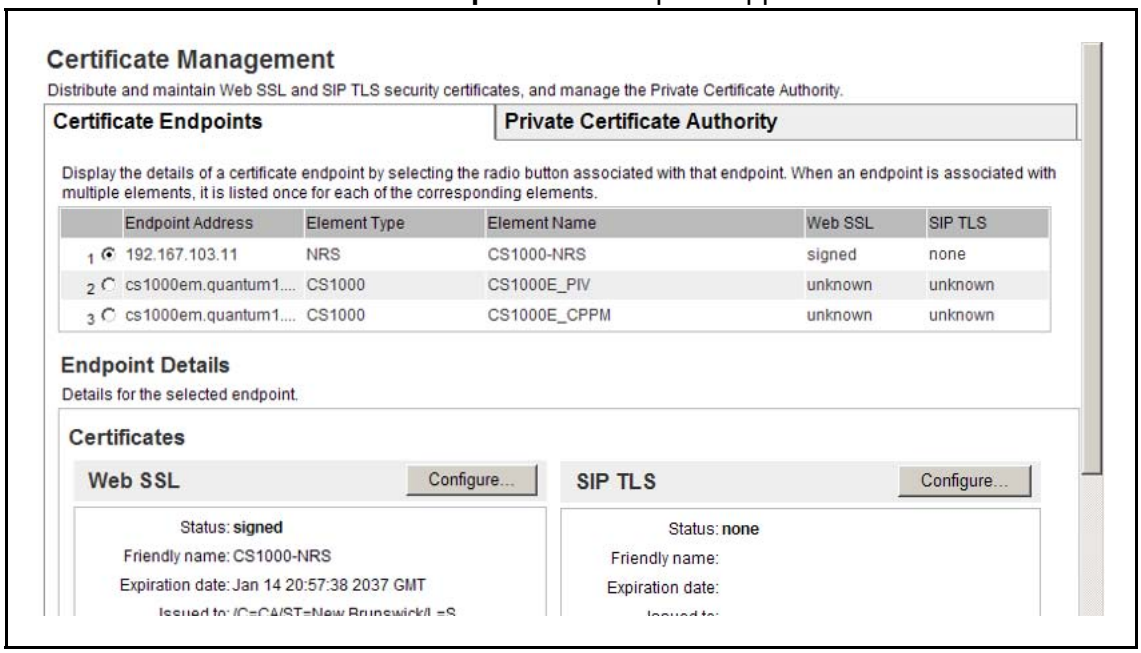
2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



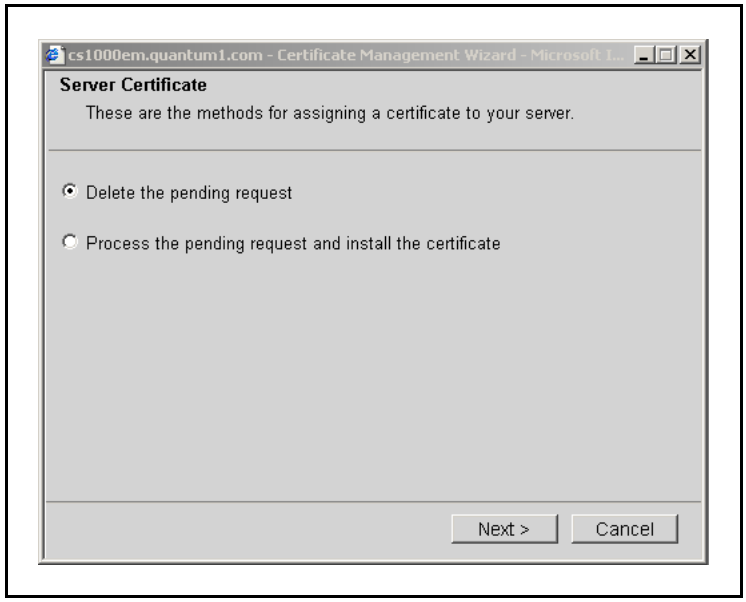
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure.

The **Endpoint Details** pane appears.



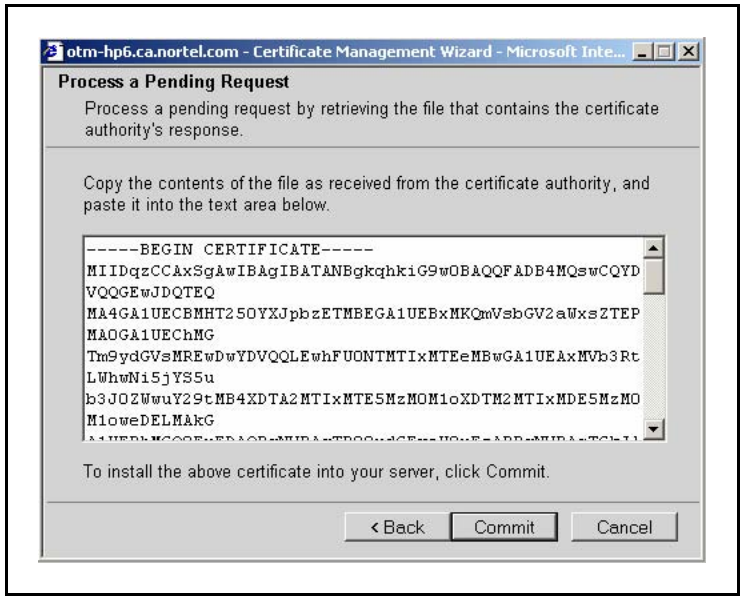
4 In the **Web SSL** or **SIP TLS** pane, click **Configure**; the certificate endpoint status must be pending or pending renew.

The **Server Certificate** window appears.



5 Select **Process the pending request and install the certificate**, and click **Next**.

The **Process a Pending Request** window appears.



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

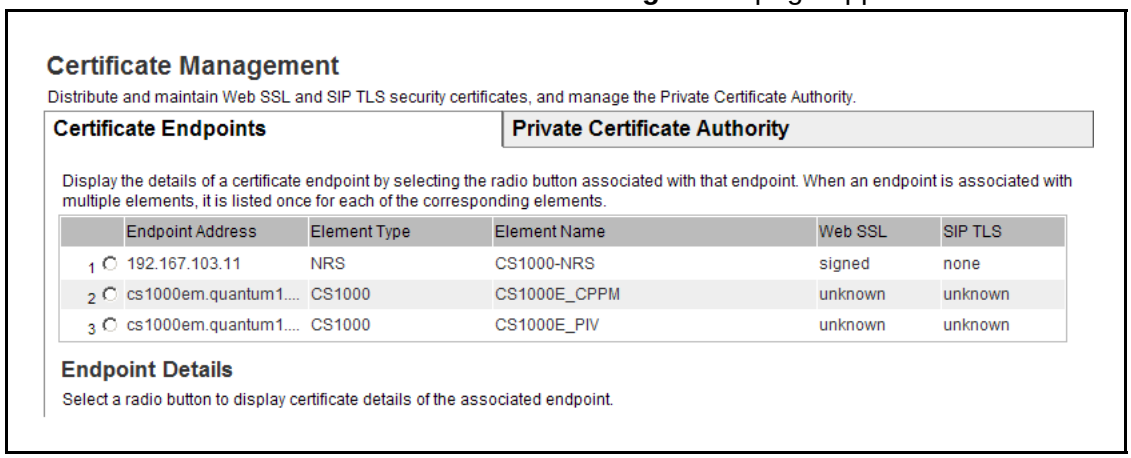
Use the following procedure to delete a pending certificate request.

Prerequisites

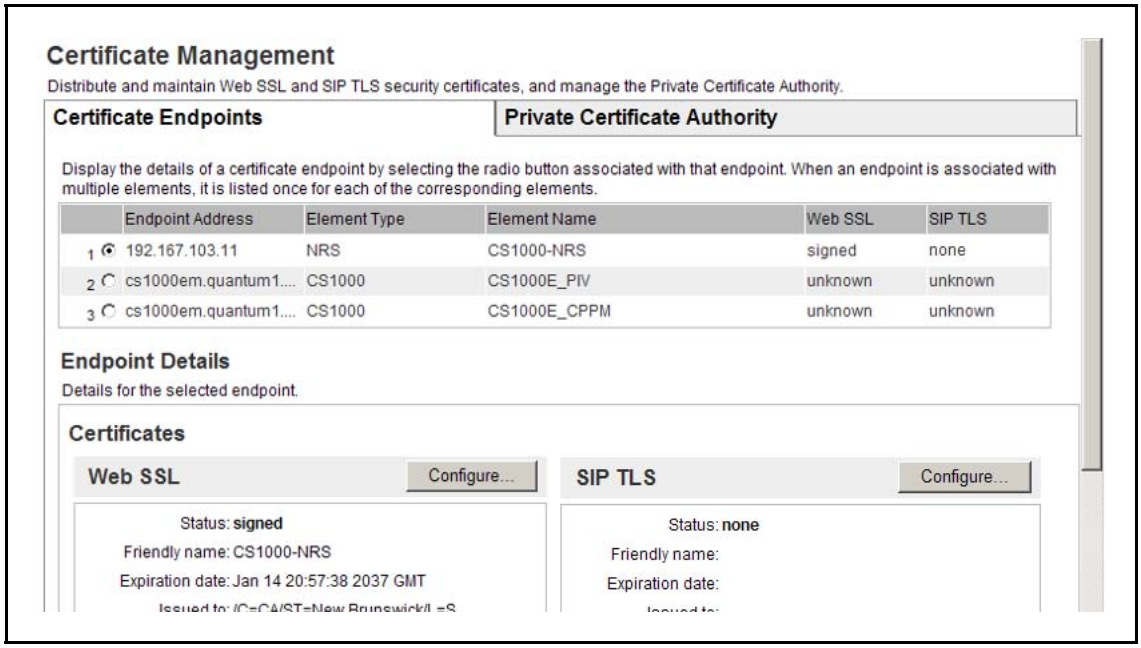
- Before you delete a pending certificate request, ensure that the certificate endpoint status is pending. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 52
Deleting a pending certificate request by using ECM

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

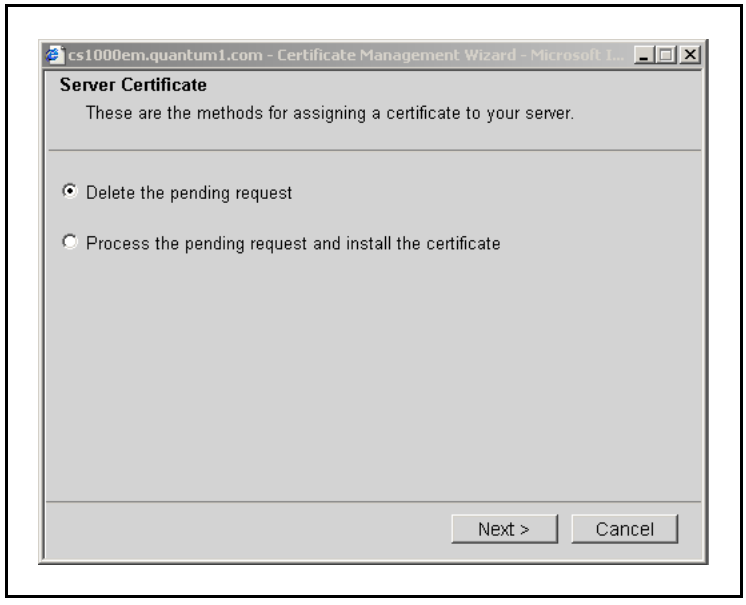


3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears.



4 In the **Web SSL** or **SIP TLS** section, click **Configure**; the certificate endpoint status must be pending or pending renew.

The **Server Certificate** window appears.



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.

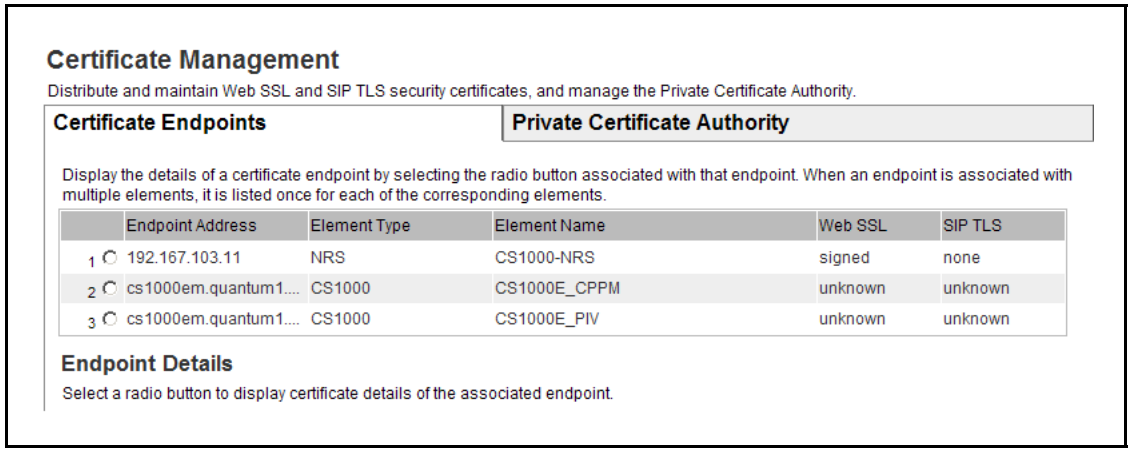
Use the following procedure to create a certificate renewal request.

Prerequisites

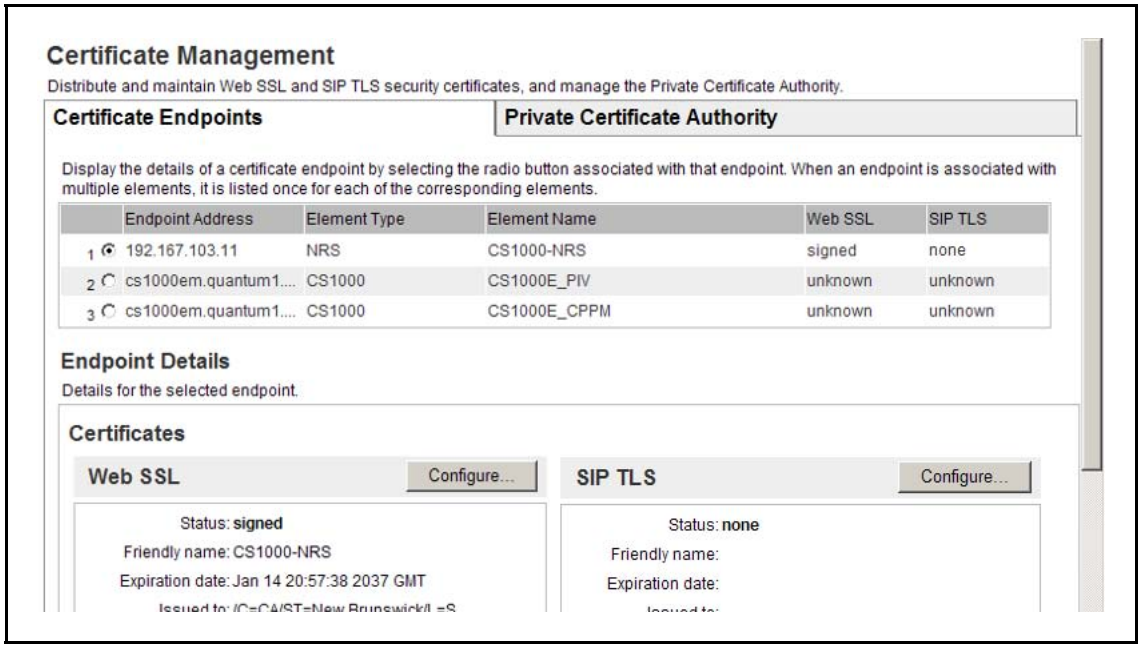
- Before you request a certificate renewal, ensure that the certificate endpoint status is signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 53
Creating a certificate renew request by using ECM

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

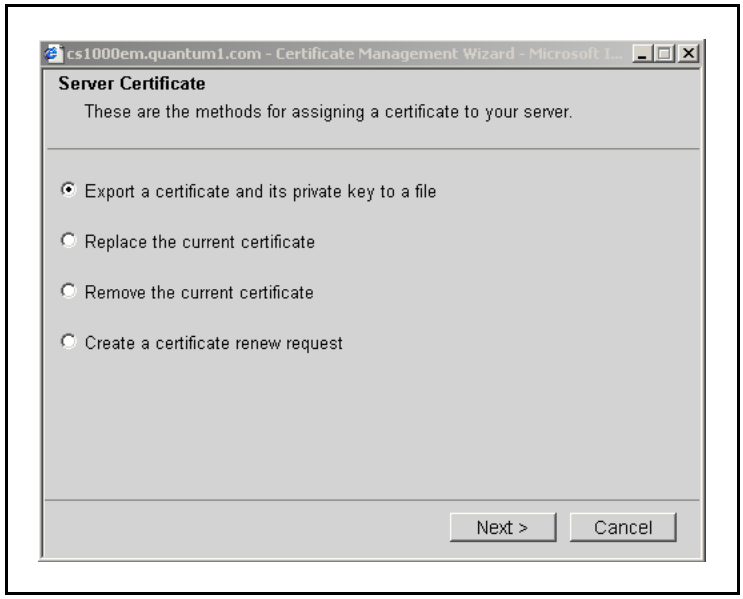


3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears.



4 In the **Web SSL** or **SIP TLS** section, click **Configure**.

The **Server Certificate** window appears.

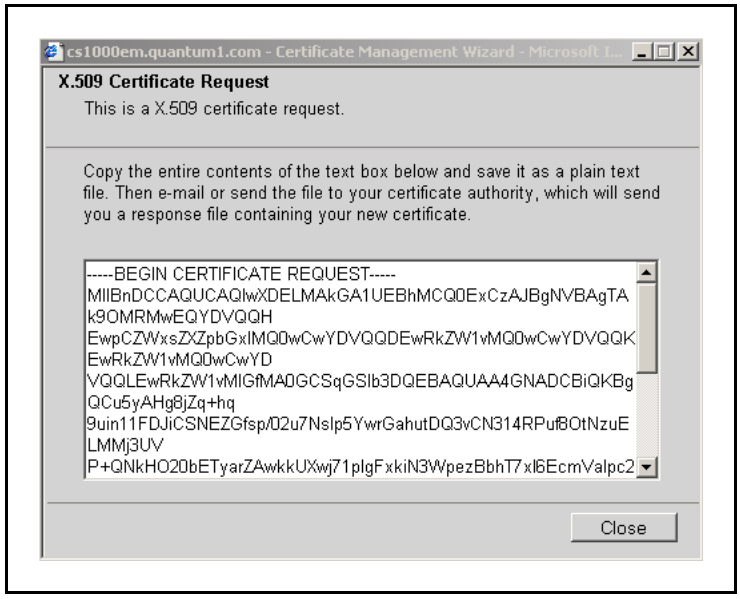


5 Select **Create a certificate renew request**, and click **Next**.

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.



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.

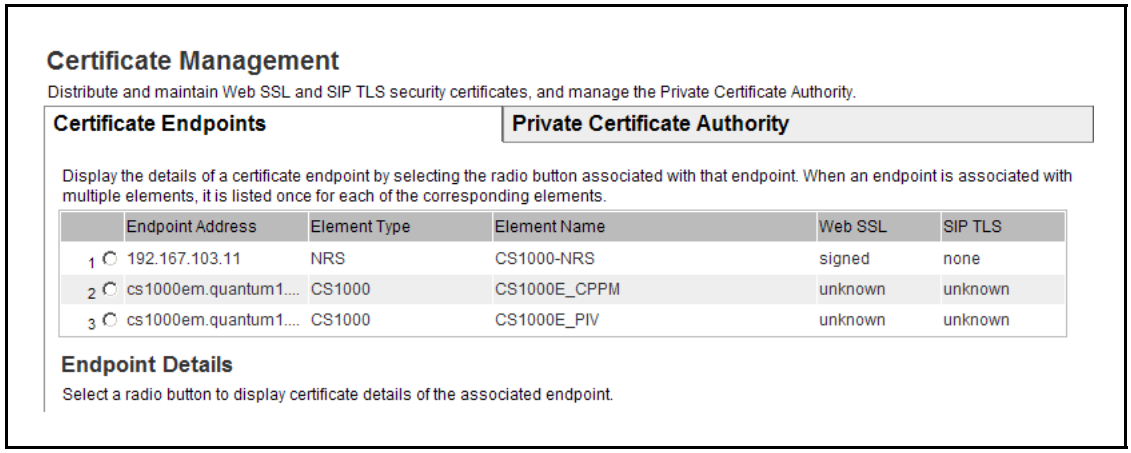
Use the following procedure to export the current self-signed certificate.

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 39 "Status types for certificate endpoints" (page 132).

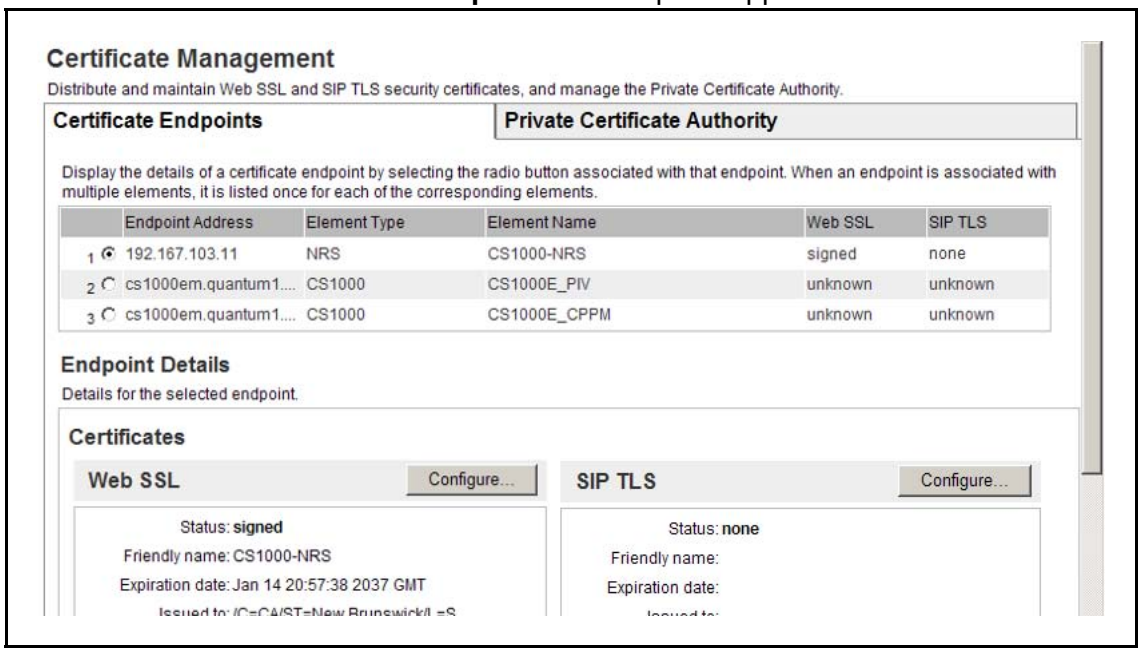
Procedure 54
Exporting the current self-signed certificate by using ECM

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



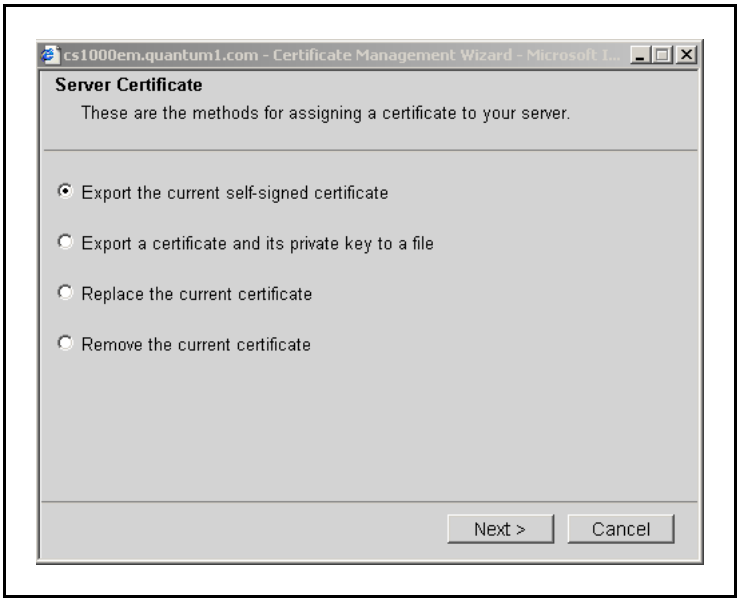
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure.

The **Endpoint Details** pane appears.



4 In the **Endpoint Details** pane, click **Configure** next to either **Web SSL** or **SIP TLS**.

The **Server Certificate Configuration Wizard** window appears.



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 183).

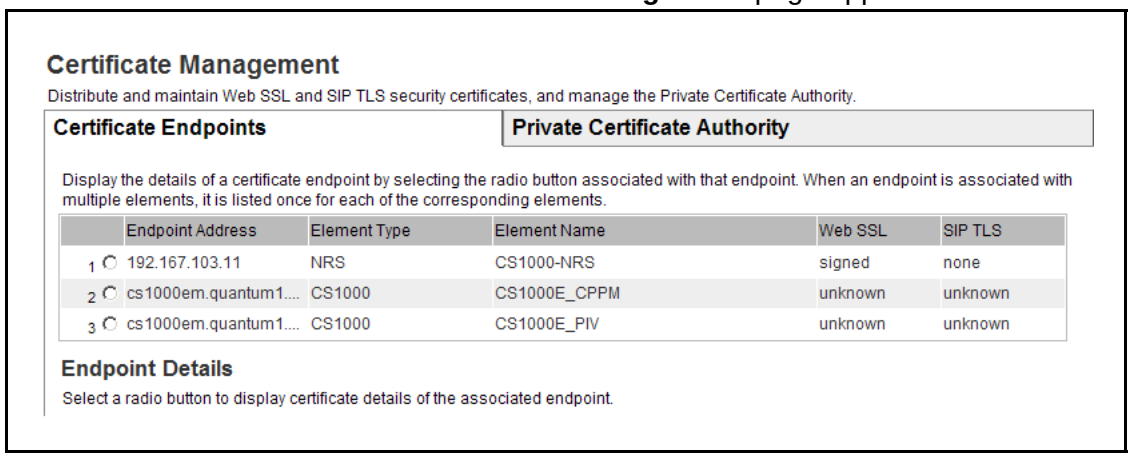
Use the following procedure to export the current certificate and its private key.

Prerequisites

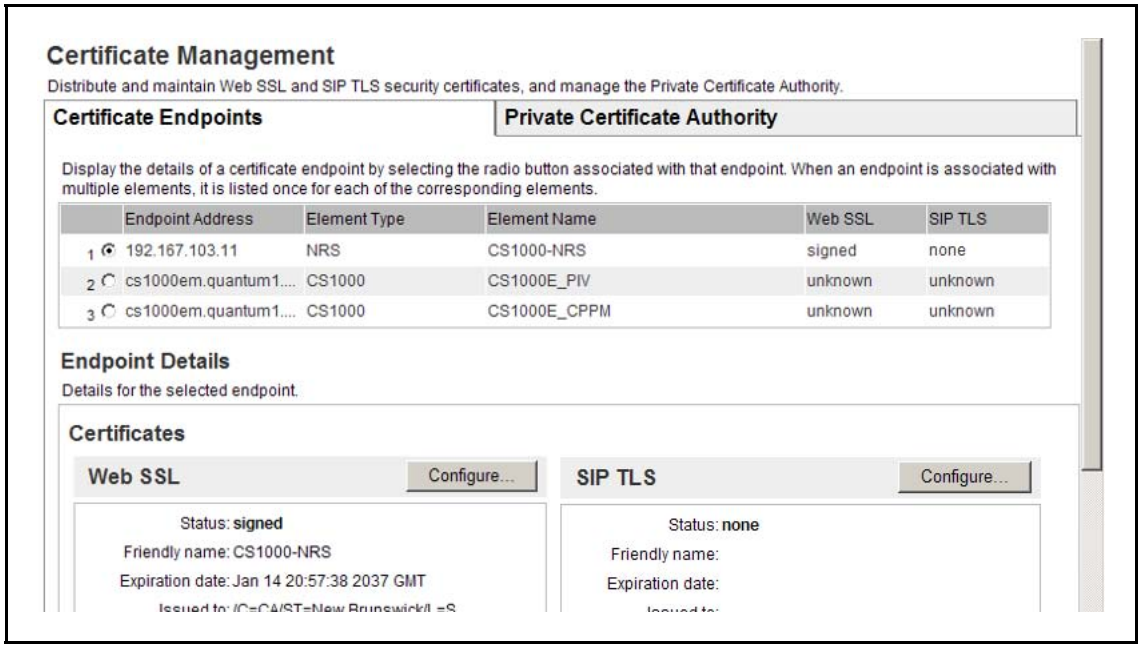
- Before you export the current certificate and its key, ensure that the certificate endpoint status is one of: self-signed, signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 55
Exporting the current certificate and its private key by using ECM

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



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint from which you want to export the certificate and key. The **Endpoint Details** pane appears.

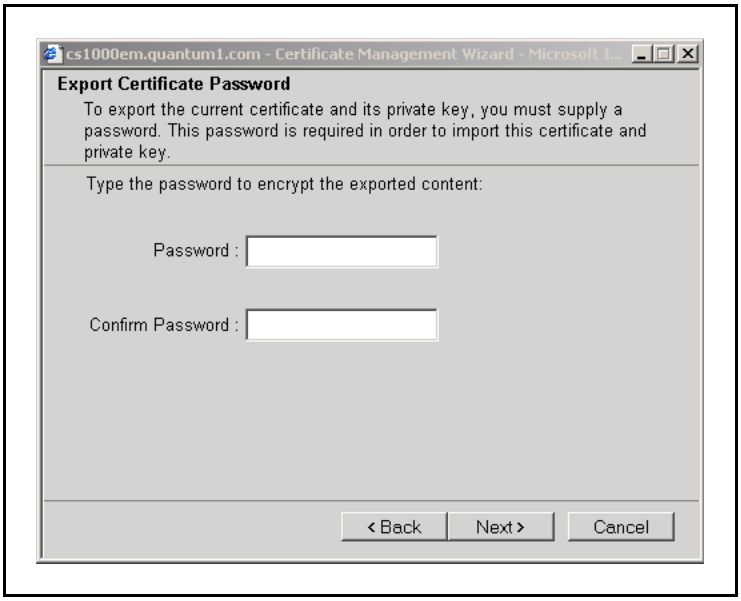


4 In the **Web SSL** or **SIP TLS** pane, click **Configure**.

The **Server Certificate** window appears.

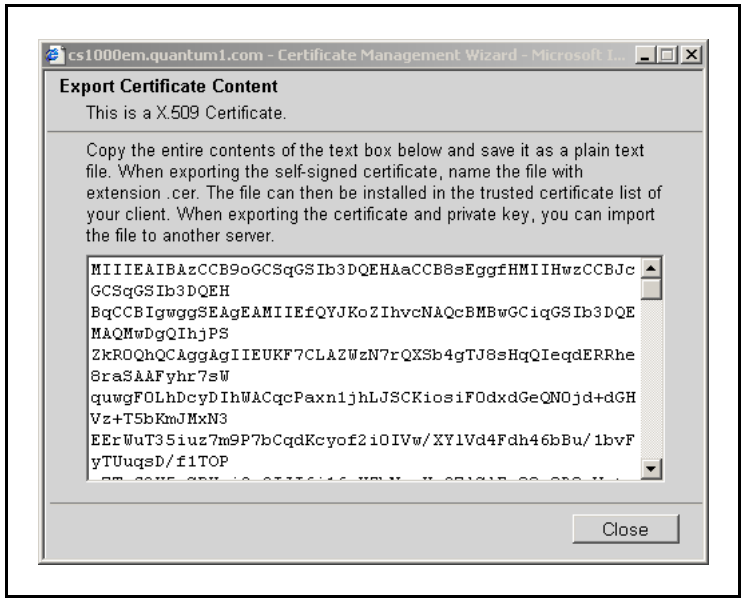
5 Select **Export a certificate and its private key to a file**, and click **Next**.

The **Export Certificate Password** window appears.



6 Enter the password in the *Password* and *Confirm Password* fields, and click **Next**.

The **Export Certificate Content** window appears.



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 180). When you import the certificate and key, you must enter the same certificate password that you entered when you exported the certificate and key.

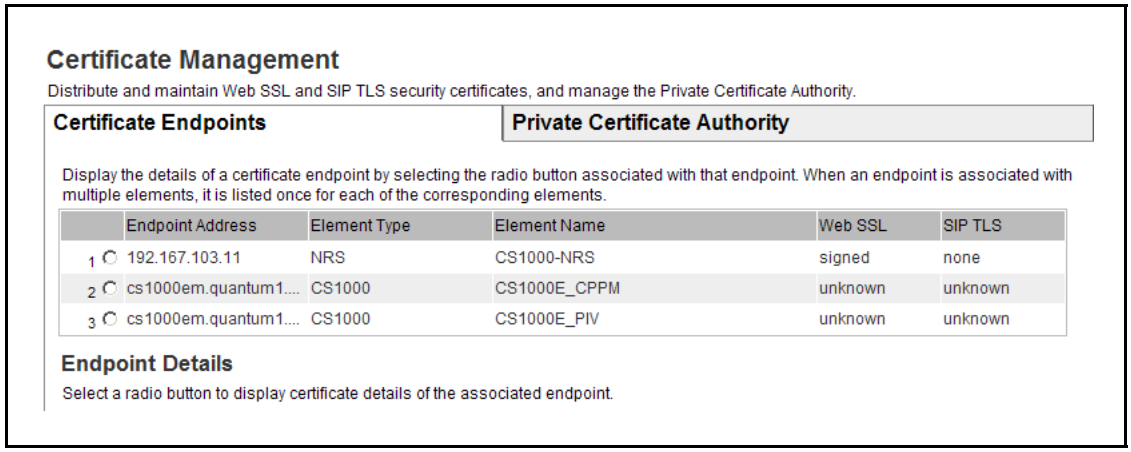
Use the following procedure to import a certificate and its private key to an endpoint.

Prerequisites

- Before you can complete the steps in this procedure, you must export a certificate and its key using the steps in Procedure 55 “Exporting the current certificate and its private key by using ECM” (page 181), 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 39 "Status types for certificate endpoints" (page 132).

Procedure 56
Importing a certificate and its private key from a file by using ECM

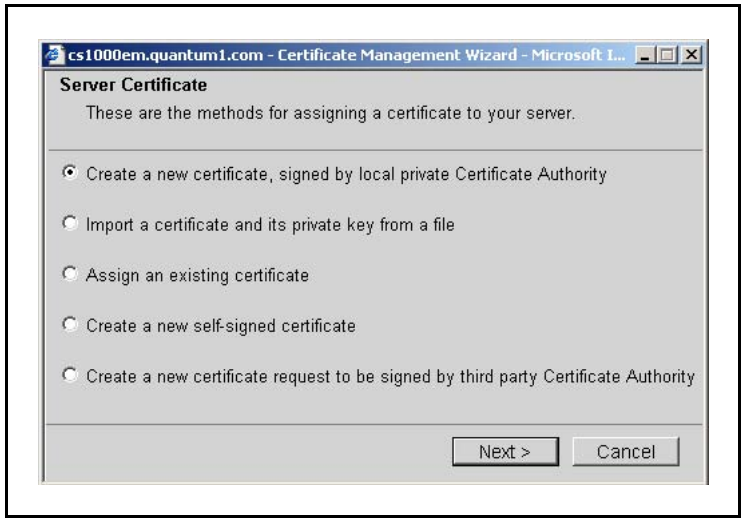
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears.



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint to which you want to import the certificate and key. The **Endpoint Details** pane appears.

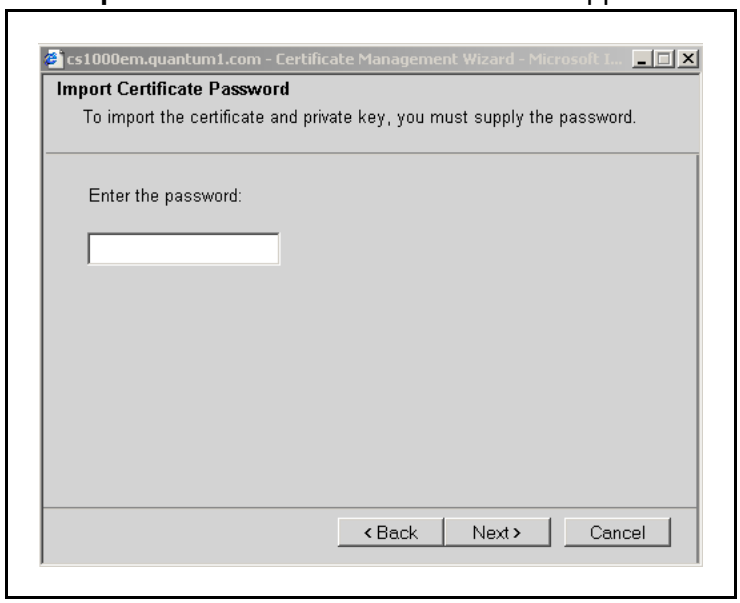
4	In the **Web SSL** or **SIP TLS** section, click **Configure**.

The **Server Certificate** window appears.



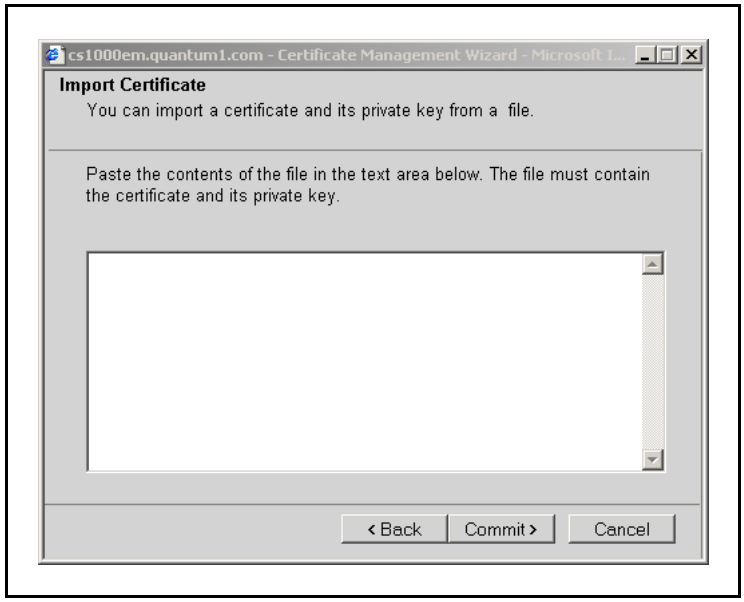
5 Select **Import a certificate and its private key from a file**, and click **Next**.

The **Import Certificate Password** window appears.



6 Enter the password of the certificate file, and click **Next**.

The **Import Certificate** window appears.



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 55 “Exporting the current certificate and its private key by using ECM” (page 181).

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

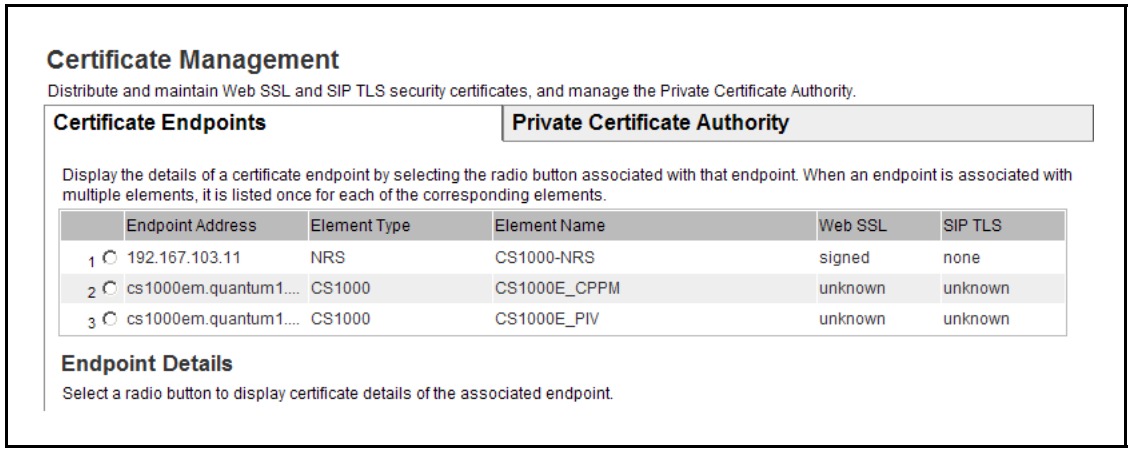
- Before you assign an existing certificate to an endpoint, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 57
Assigning an existing certificate by using ECM

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

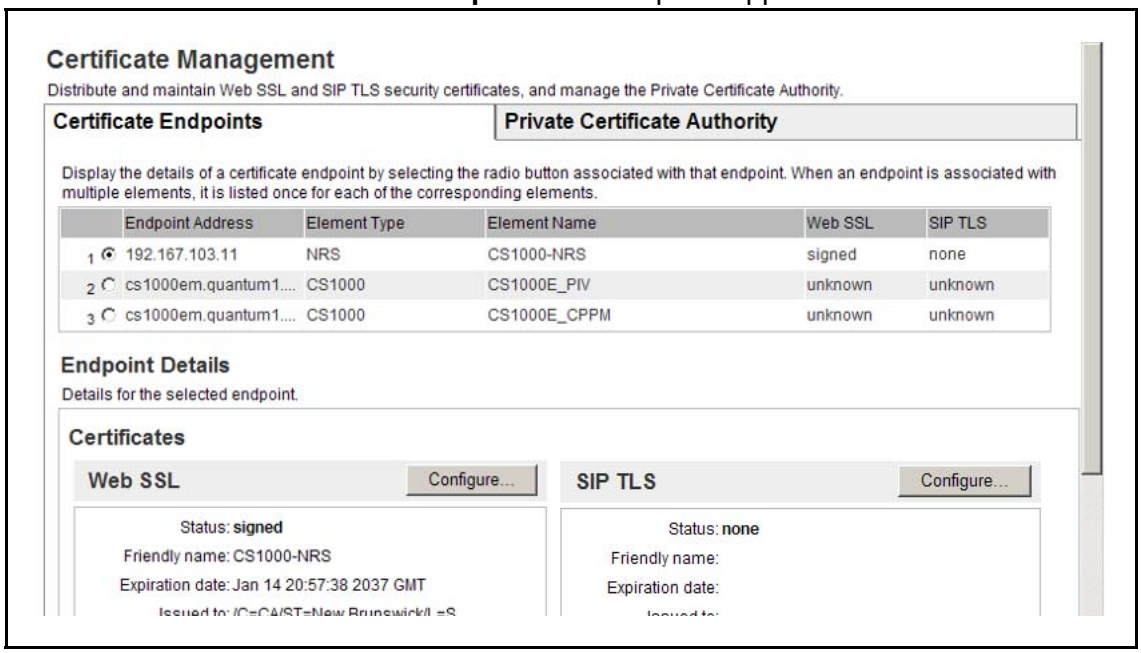
2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



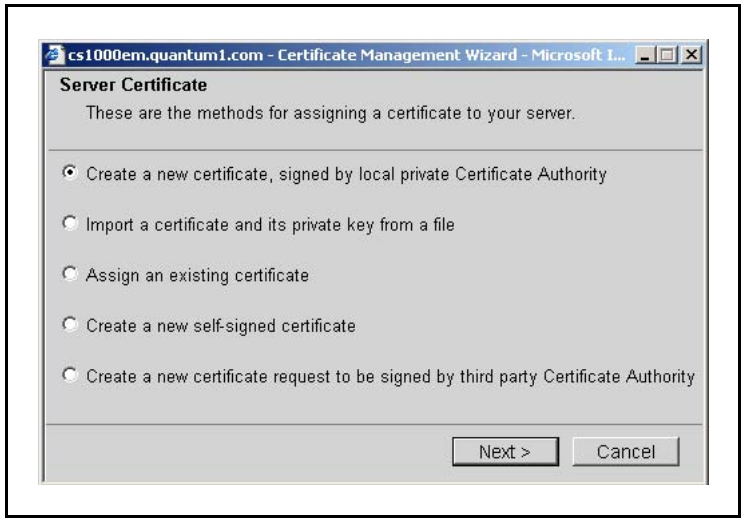
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure.

The **Endpoint Details** pane appears.



4 In the **Endpoint Details** pane, click **Configure** next to either **Web SSL** or **SIP TLS**.

The **Server Certificate** window appears.



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

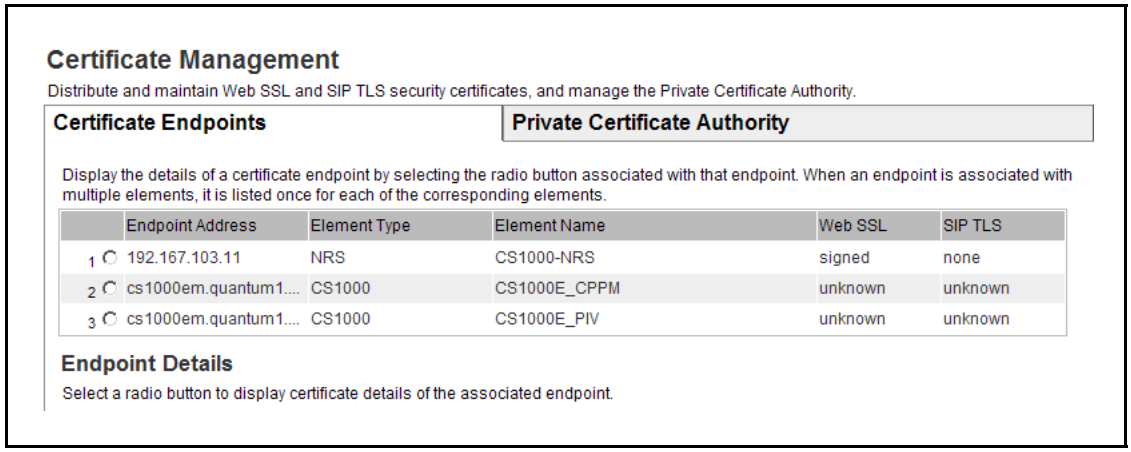
- You can replace a certificate only if more than one certificate is configured.
- Before you replace the current certificate, ensure that the certificate endpoint status is one of: signed, self-signed, expired, or about to expire. For more information about certificate endpoint status types, see Table 39 "Status types for certificate endpoints" (page 132).

Procedure 58
Replacing the current certificate by using ECM

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

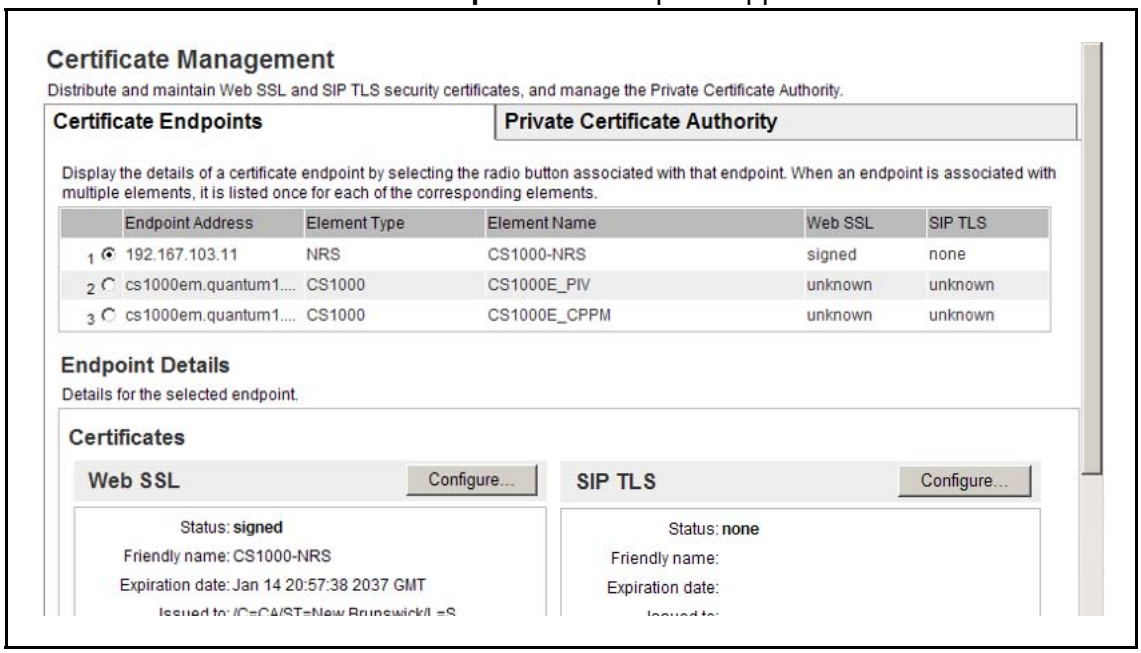
2 Click **Security** > **Certificates**.

The **Certificate Management** page appears.



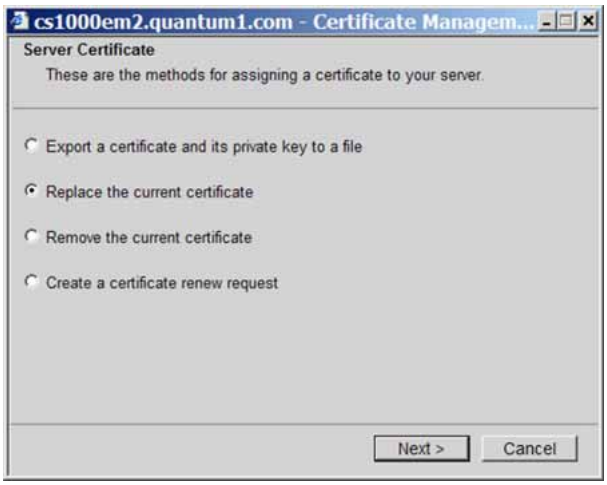
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint that you want to configure.

The **Endpoint Details** pane appears.



4 In the **Web SSL** or **SIP TLS** section, click **Configure**.

The **Server Certificate** window appears.



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.

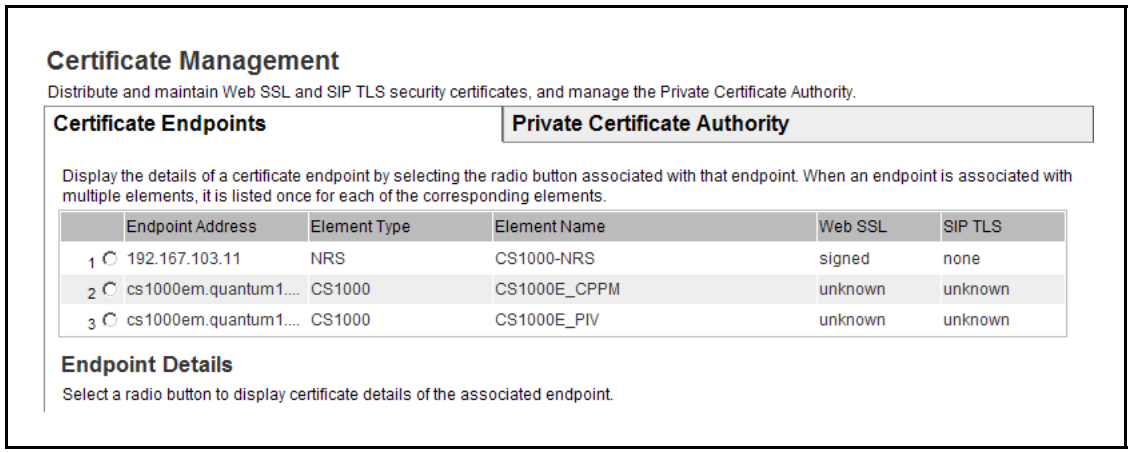
Prerequisites

- 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 39 "Status types for certificate endpoints" (page 132).

Procedure 59
Removing the current certificate by using ECM

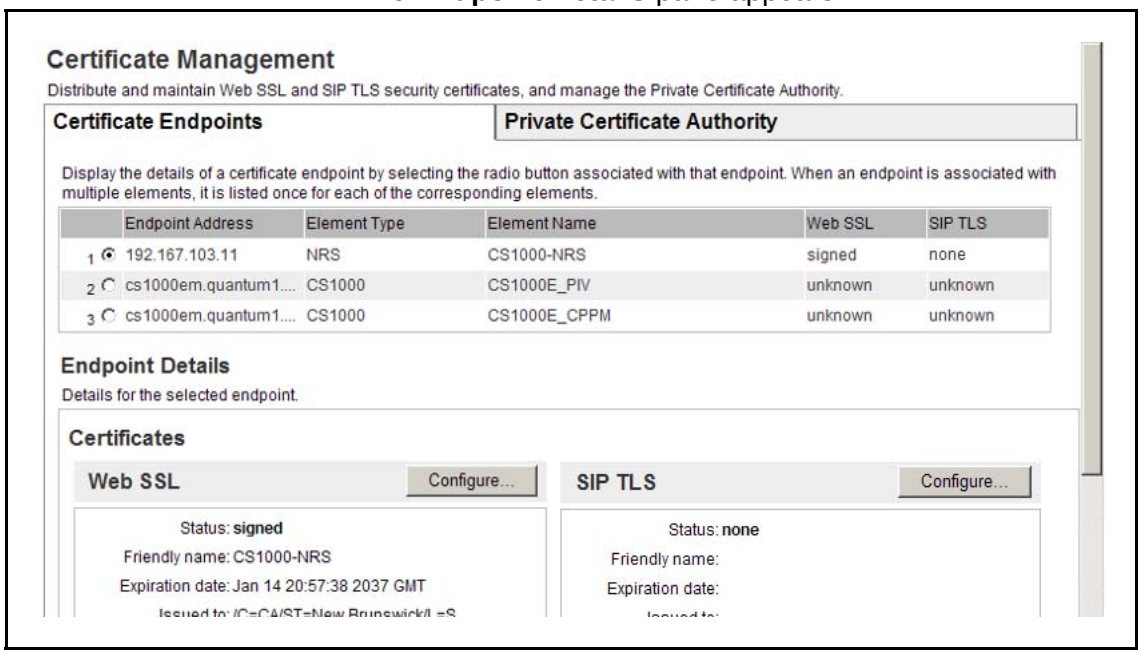
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**.

The **Certificate Management** page appears.



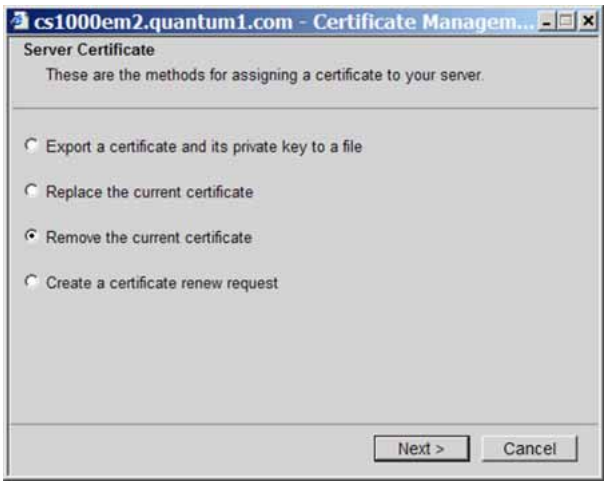
3 In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure.

The **Endpoint Details** pane appears.



4 In the **Web SSL** or **SIP TLS** section, click **Configure**.

The **Server Certificate** window appears.



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--

SIP security

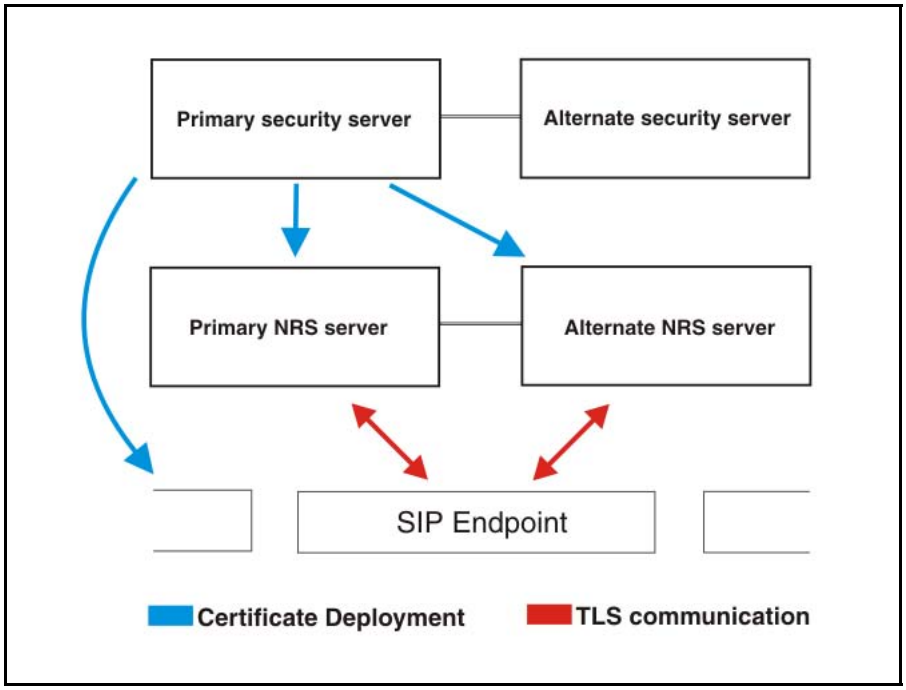
This chapter contains procedures to help you protect Session Initiation Protocol (SIP) signaling by using Transport Layer Security (TLS). The chapter is divided into the following sections:

About TLS security for SIP trunks

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 (CS 1000), see “TLS security for SIP trunks concepts” (page 33).

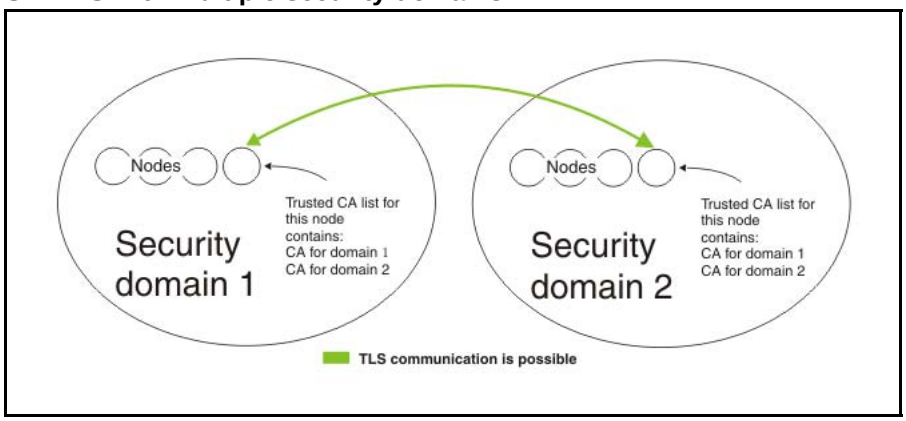
Certificates are deployed from the primary security server to the primary and secondary NRS servers and to the SIP endpoints. TLS communication can then be enabled between the active NRS server and the SIP endpoints. For an illustration of the distribution of certificates and subsequent TLS communication within a security domain, see Figure 2 "SIP TLS with one security domain" (page 194).

Figure 2
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 Figure 3 "SIP TLS with multiple security domains" (page 194).

Figure 3
SIP TLS with multiple security domains



SIP TLS configuration overview

A typical deployment of a SIP-enabled CS 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 ECM that is the primary security server, and all the NRS must be members of the ECM community of trust of that primary ECM security Sever.

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 ECM, add a new element by using the steps in Procedure 2 "Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements" (page 57).
   - In ECM, create a certificate by using the steps in one of the following:
     - "Create a certificate for SIP TLS signed by the private CA " (page 150)
     - "Create a certificate for SIP TLS signed by a public CA " (page 155)
     - "Create a self-signed certificate for SIP TLS " (page 167)
   - If the system has a secondary NRS with SIP Proxy and Redirect server:
     - In ECM, 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 180).
     - In ECM, 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 183).
     - In ECM, add a CA to the service, and paste the certificate information by using the steps in "Add a CA to an endpoint" (page 128).
2. Enable TLS for SIP Proxy and Redirect server
   - If there is a firewall between the ECM 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 389 for LDAP
- 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 ECM, provision a public-key certificate for the primary SIP Proxy and Redirect server
- In ECM, 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 Installation and Commissioning (NN43001-564)* () .
- Restart the SIP Proxy service.

3. Deploy certificates for SIP endpoints

— In ECM, add a new element (of type gateway) for each signaling server that is a leader or follower (and thus could become active as a SIP gateway) by using the steps in Procedure 2 “Adding a CS 1000 Release 5.0 or Release 5.5 system to the list of ECM managed elements” (page 57).

— In ECM, create a certificate by using the steps in one of the following:

- “Create a certificate for SIP TLS signed by the private CA ” (page 150)
- “Create a certificate for SIP TLS signed by a public CA ” (page 155)
- “Create a self-signed certificate for SIP TLS ” (page 167)

— If the system has other signaling servers running standby SIP services, you must perform the following steps for each signaling server:

- In ECM, 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 180).
- In ECM, 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 183).
- In ECM, add a CA to the service, and paste the certificate information by using the steps in “Add a CA to an endpoint” (page 128).

4. Enable TLS for SIP endpoints

— If there is a firewall between the ECM 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 389 for LDAP
- TCP port 636 for LDAPS
- TCP port 15080 for Xmsg

— For SIP endpoints that use a static IP address:

- If the CS 1000 system to which the SIP gateway belongs has an ISSS security level of Full, Functional, or Optimized, then complete the following steps before you provision a certificate for the SIP gateway:
  - Using overlay 117, add the IP addresses of both eth0 and eth1 of ECM primary security server onto the IPsec target list of the CS 1000 call server. For more information about creating an ISSS target, see Procedure 20 “Creating an ISSS target by using LD 117” (page 109).
  - Configure ISSS/IPsec on ECM primary security server for the SIP endpoint. For more information, see “First-time configuration and activation of ISSS” (page 48).

- Use Element Manager to ensure that the IPsec channel between the primary security server and the SIP gateway is enabled.
- If the following error message appears, log on to Element Manager, and click on the certificate endpoint:
  The endpoint request could not be completed. Please ensure that the endpoint is online, is included in the security domain, and is set to the correct endpoint type. Refer to the logs for additional details.

- In NRS Manager, configure the SIP endpoints by using the information in *Network Routing Service Installation and Commissioning (NN43001-564)* () .

— 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 200).

Use the command line interface (CLI) commands in "SIP TLS maintenance using CLI" (page 209) 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 60
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 198).

--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 40 "SIP TLS security parameters" (page 199).

Table 40
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 41 "Job aid: SIP TLS security policy descriptions" (page 204).
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.
clientAuthentication Enabled (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.

Table 40
SIP TLS security parameters (cont'd.)

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

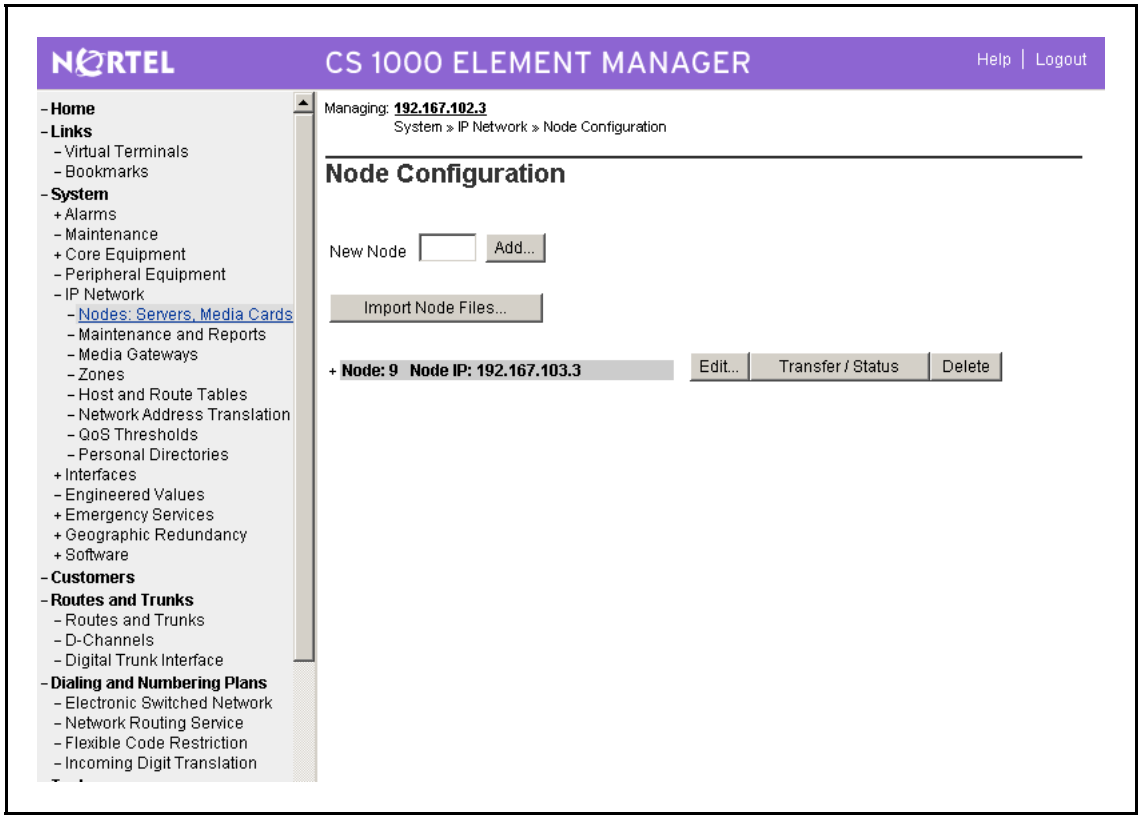
Use the procedures in this section to configure SIP TLS using Element Manager.

Configuring SIP TLS security policy

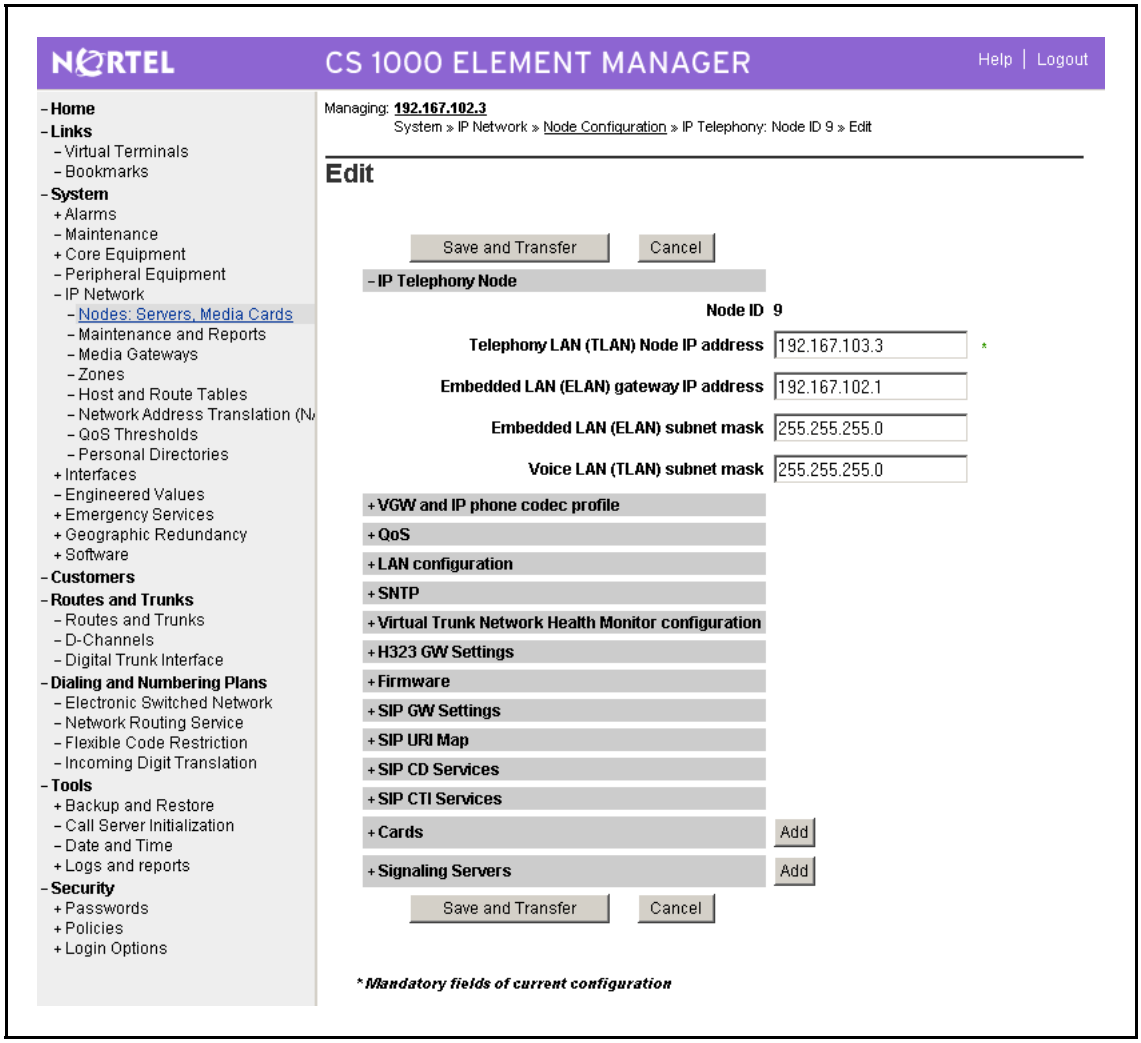
Use the procedures in this section to configure system-wide SIP TLS security policies.

Procedure 61
Configuring the system-wide TLS Security Policy by using Element Manager

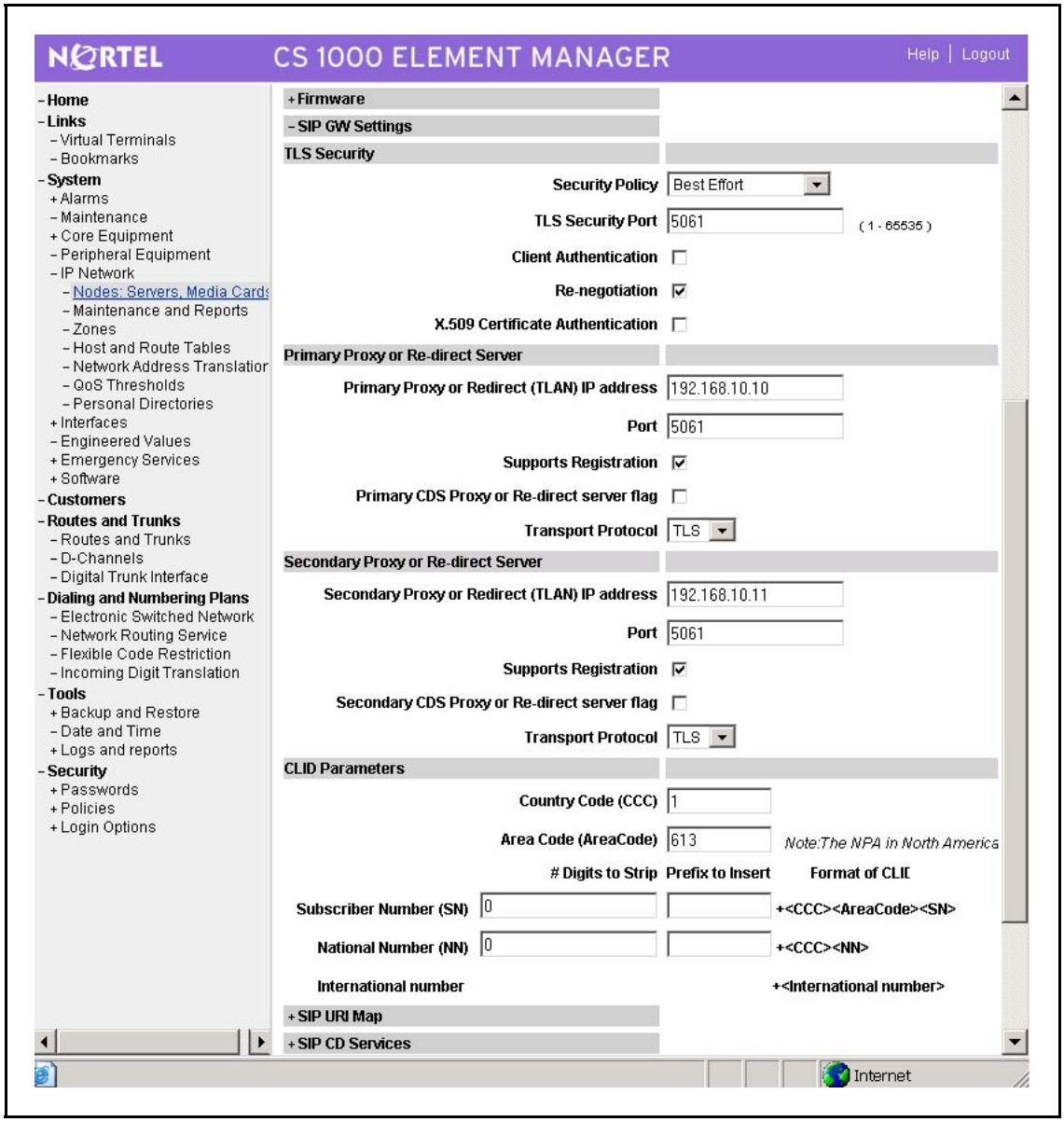
Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears.



3 Click **Edit**.
The **Edit Node** page appears.



4 Expand the **SIP GW Settings** option.



5 In the **TLS Security** section, use the **Security Policy** menu to choose one of:

- **Best effort**
- **Secure Local**
- **Secure End to End**

For more information about available security policies, see Table 41 "Job aid: SIP TLS security policy descriptions" (page 204).

6 In the **TLS Security Port** field, type `5061`.

For more information about TLS parameters, see Table 40 "SIP TLS security parameters" (page 199).

7 Verify that the **Re-negotiation** option button is selected.

8 Optionally, select the **X509 Certificate Authentication** option button to enable X509 Certificate Authentication.

> **ATTENTION**
> If you select X509 Certificate Authentication, you cannot use self-signed certificates with SIP TLS.

9 Optionally, select the **Client Authentication** option button to enable Client Authentication.

10 In the **Primary Proxy** section, type `5061` in the **Port** field, and configure **Transport Protocol** to **TLS**.

11 In the **Secondary Proxy** section, type `5061` in the **Port** field, and configure **Transport Protocol** to **TLS**.

12 Click **Save and Transfer**.

The following warning appears:
`Please reboot the following Signaling Server after the save and transfer is done: <list of SIP enabled Signaling Servers IPs>.`

13 Click **OK**.

--End--

The security policy options for SIP TLS are described in Table 41 "Job aid: SIP TLS security policy descriptions" (page 204).

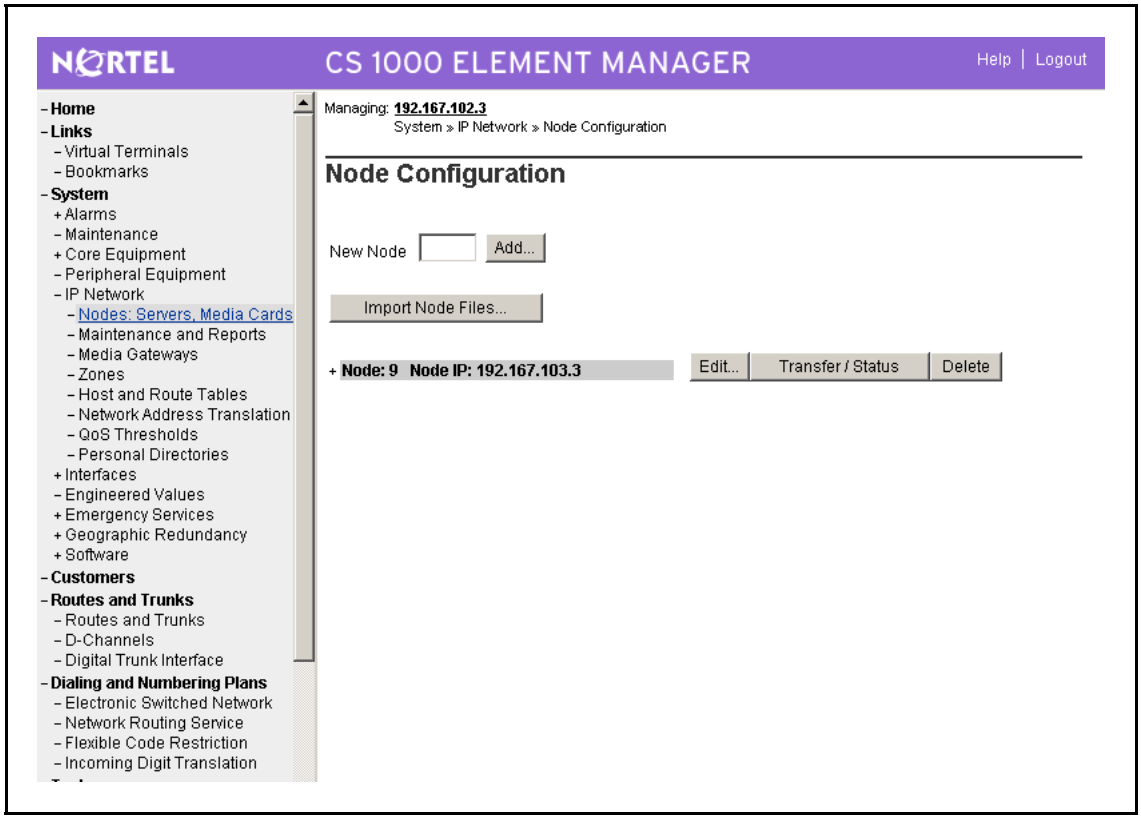
Table 41
Job aid: SIP TLS security policy descriptions

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.

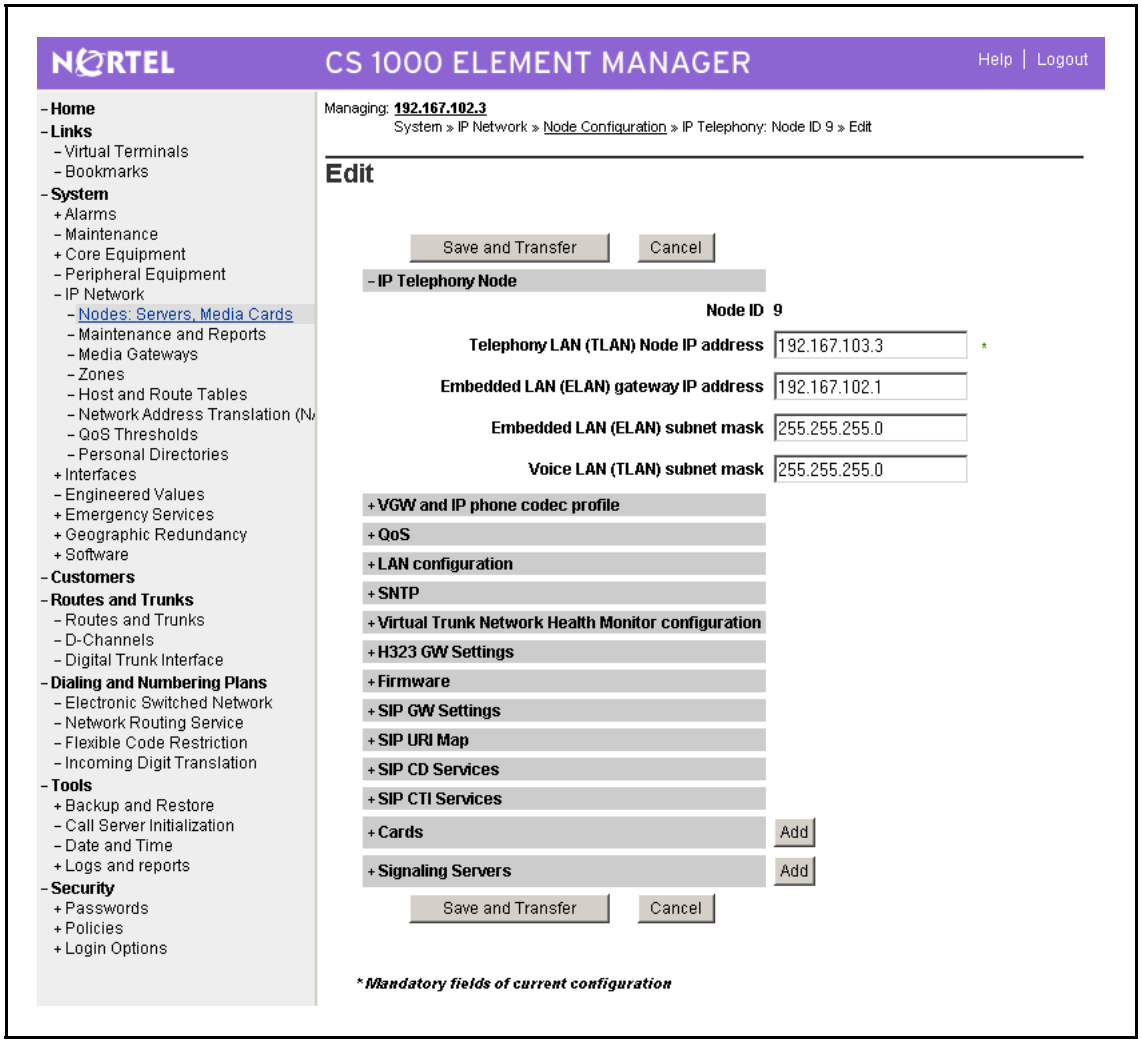
Secure Local (Guarantee local hop TLS)	Secure Local turns SIP TLS on. SIP Gateway will listen only on its TLS port. Transport protocol to SIP Proxy and Redirect Server on Linux can only be TLS. SIP Redirect Server on VxWorks is not supported as the next hop of this SIP Gateway. SIP URI scheme is SIP.
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 62
Disabling SIP TLS by using Element Manager

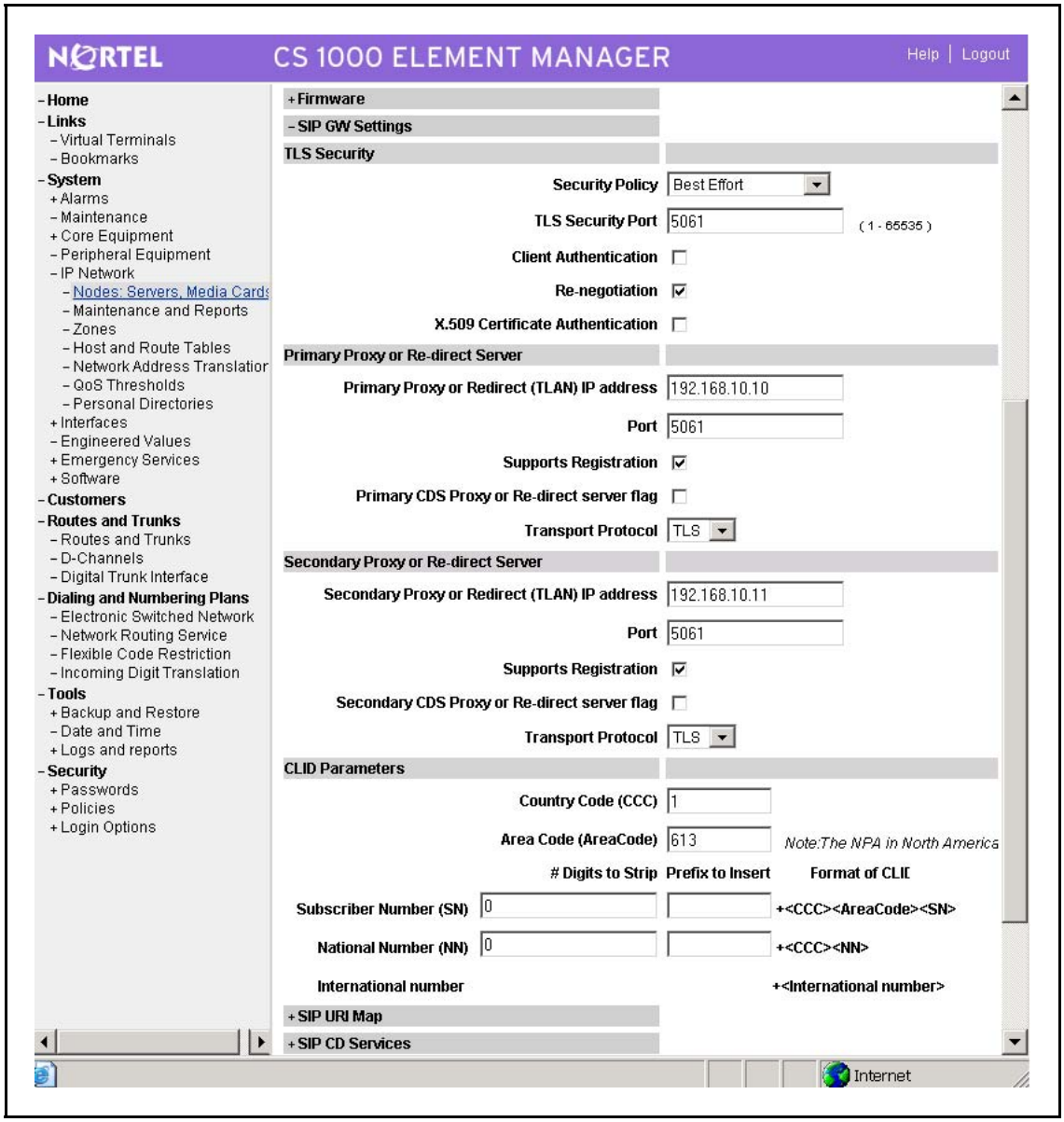
Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears.



3 Click **Edit**.
The **Edit Node** page appears.



4 Expand the **SIP GW Settings** option.



5 In the **TLS Security** section, use the **Security Policy** menu to choose **Security disabled**.

For more information about available security policies, see Table 41 "Job aid: SIP TLS security policy descriptions" (page 204).

6 Verify that the **TLS Security Port** option is disabled, and that the **Client Authentication**, **Re-negotiation**, and **X509 Certificate Authentication** check boxes are cleared.

For more information about TLS parameters, see Table 40 "SIP TLS security parameters" (page 199).

7 In the **Primary Proxy** and **Secondary Proxy** sections **Transport Protocol** menus, verify that **TCP** or **UDP** is selected.

8 Ensure that all other fields on the page are configured with values appropriate to the SIP configuration on your system.

9 Click **Save and Transfer**.

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--

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 198).

SIP TLS Certificate management

You can manage SIP TLS certificates using the Enterprise Common Manager (ECM) interface. For more information about certificate management using ECM, see "Certificate Management" (page 123).

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

Use the Media Security feature to secure media exchanges on Communication Server 1000 (CS 1000) through the use of Secure Real-time Transport Protocol (SRTP) on IP media paths. It applies to CS1000 IP clients (Phase 2 sets only) and devices using DSPs (DSP daughter board 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 CS 1000, see "Media Security concepts" (page 32).

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 42 "Configuration options available for Media Security" (page 212) shows the configuration possibilities for the Media Security feature.

Table 42
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 43 "Details of Class of Service options for Media Security" (page 212).

Table 43
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 4.5).
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.

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

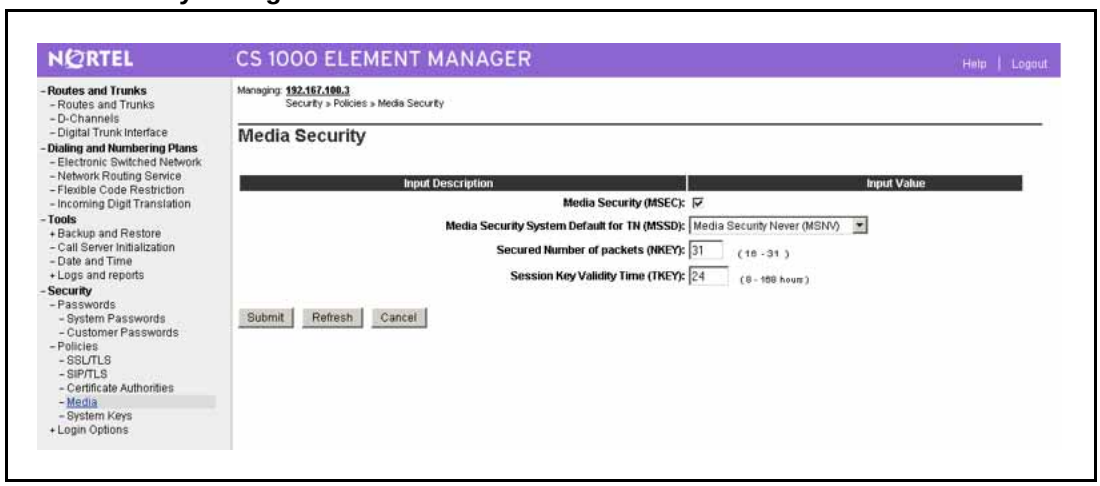
Use the procedures in this section to configure Media Security using Element Manager.

System-wide Media Security configuration

You can configure a system-wide configuration setting that controls whether or not the CS 1000 system is capable of providing Media Security. By default, Media Security is enabled on the system.

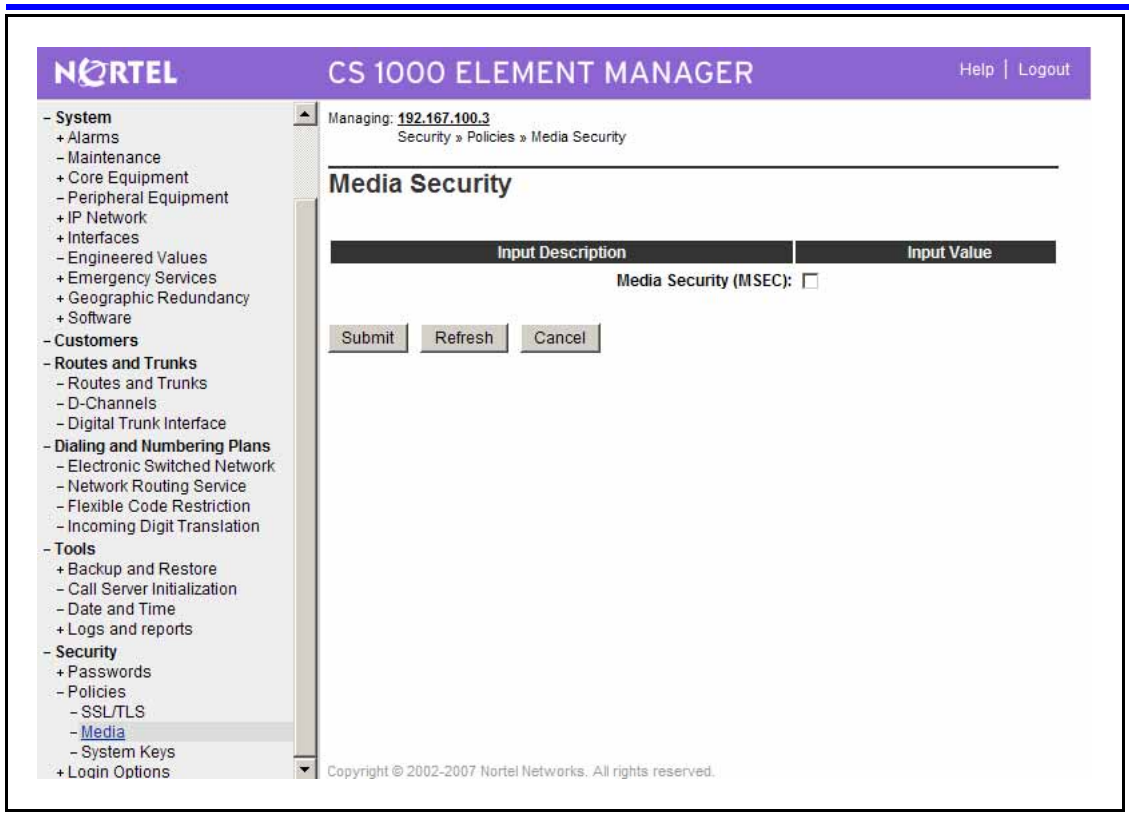
You can configure system-wide Media Security using the Media Configuration page in Element Manager, as shown in Figure 4 "Media Security configuration" (page 214). For more information about configuring Element Manager, see *Element Manager System Reference — Administration (NN43001-632)* () .

Figure 4
Media Security configuration

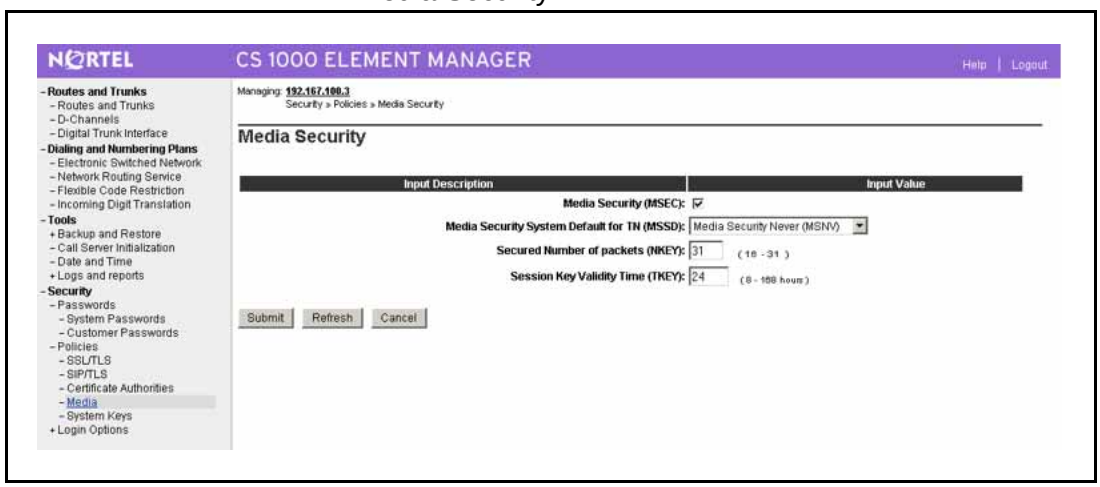


Procedure 63
Configuring system-wide Media Security by using Element Manager

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.



3 Select the **Media Security** check box to enable system-wide Media Security.



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.

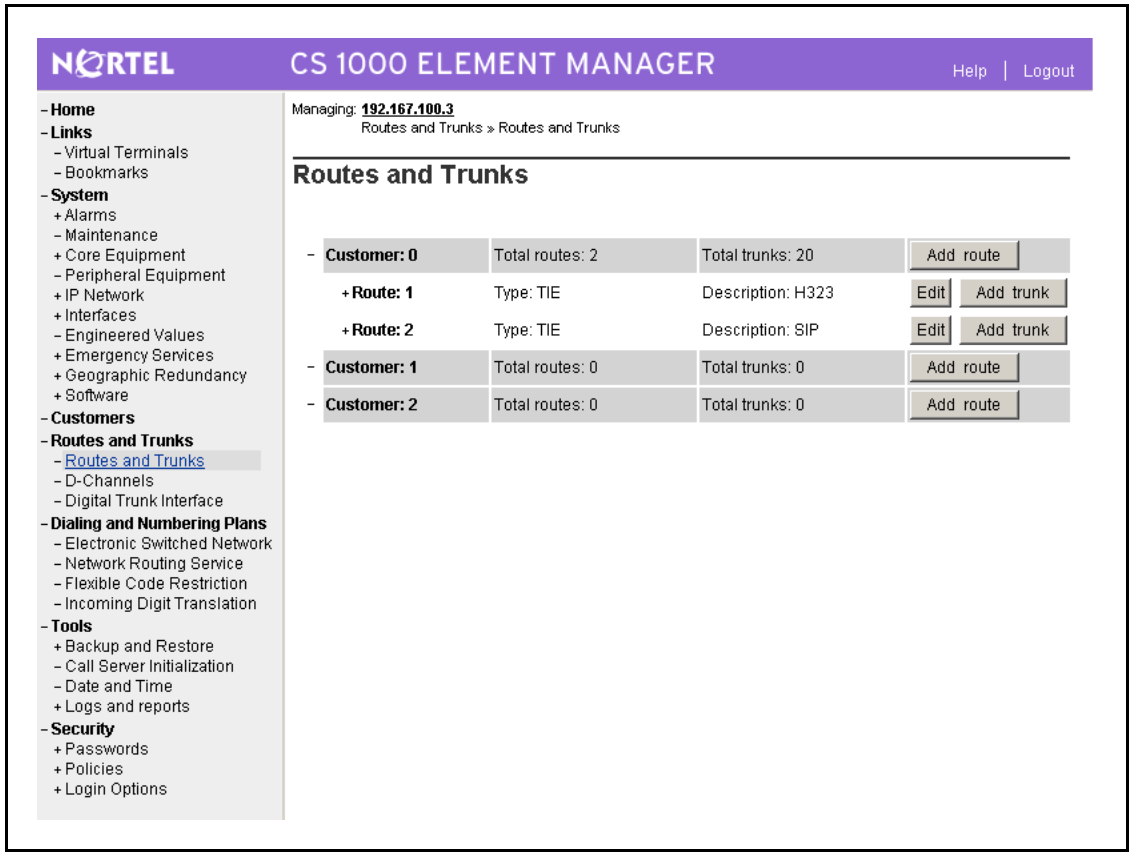
--End--

VTRK Class of Service configuration

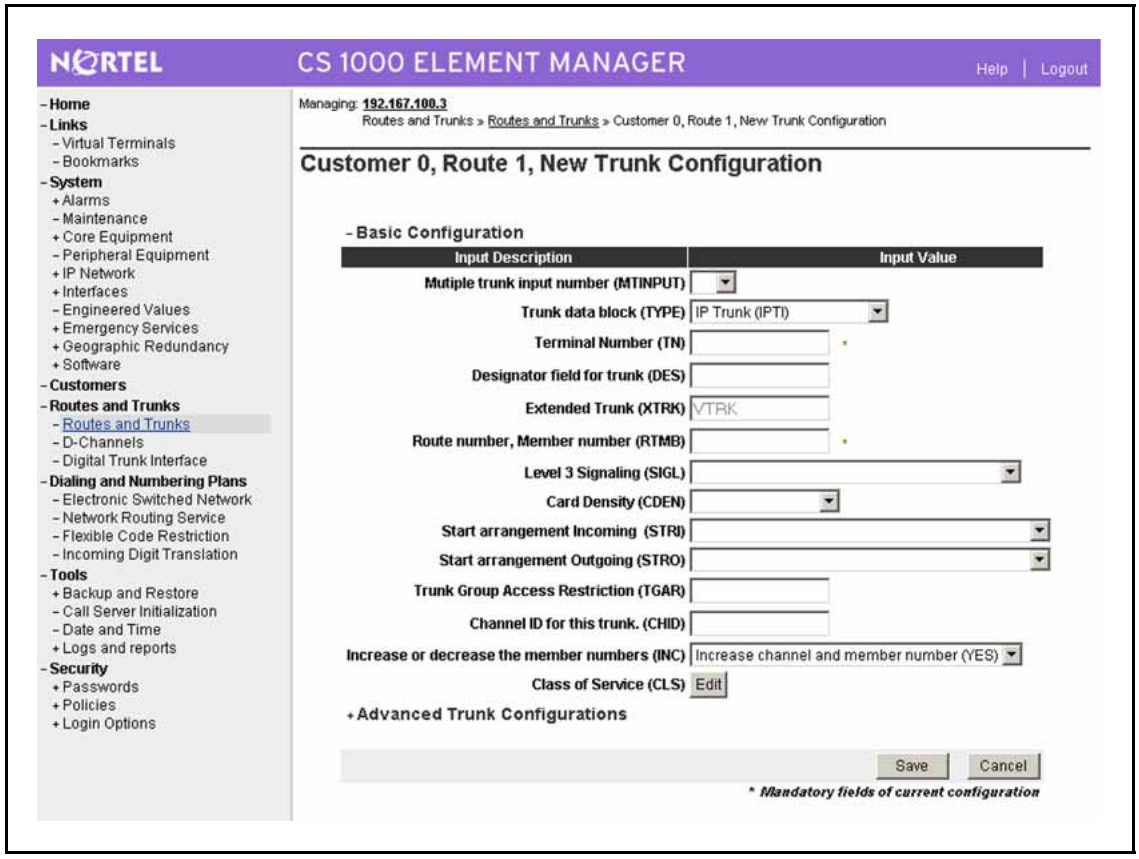
You can configure Media Security Class of Service for Virtual Trunks (trunks that have XTRK configured as VTRK).

Procedure 64
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 > Route and Trunks**, and select a customer record.



3 Click **Add Trunk** for the route to which you want to add a trunk. The New Trunk Configuration page appears.



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.

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 CS 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 65
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 44
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 66
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 219). 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 67
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 45
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 214).

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 68
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 46 "Job aid: commands to access information about Media Security configuration" (page 224).

--End--

Table 46
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

Table 46
Job aid: commands to access information about Media Security configuration (cont'd.)

		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 69
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 70
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 47
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 71
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 220).
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 72
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 229)
- “User and password management using overlays” (page 231)
- “User and password management using Element Manager” (page 251)

For more information about user and password management concepts on Communication Server 1000 (CS 1000), see “User and password management concepts” (page 39).

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 282).

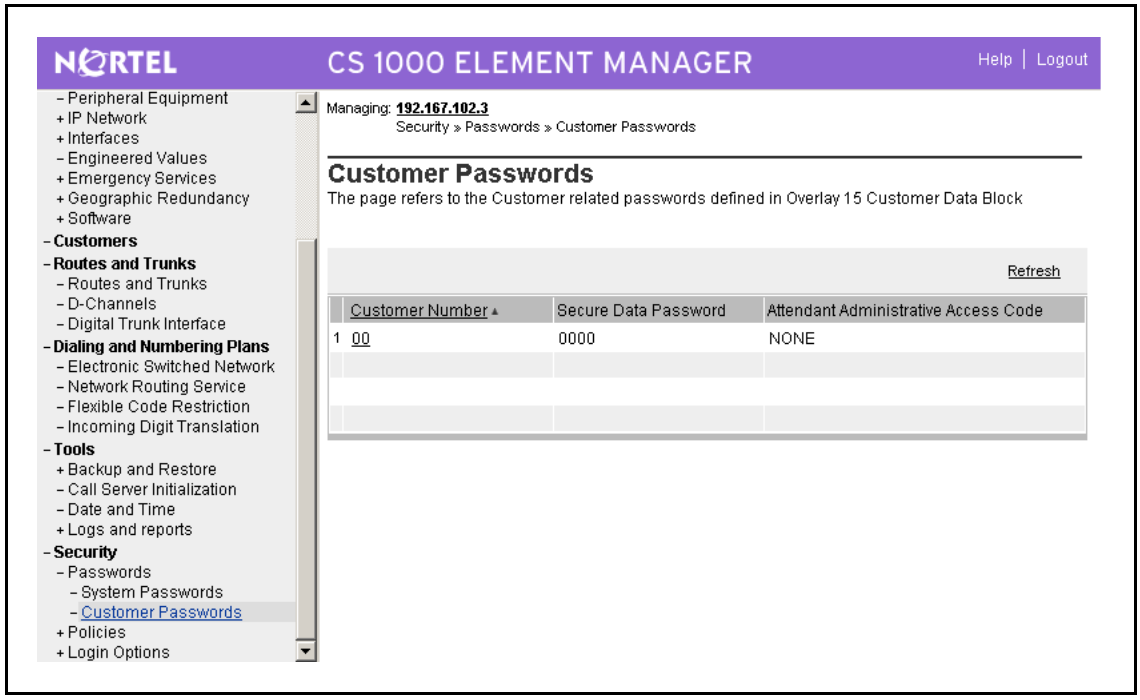
Customer passwords

For each Customer Number defined on the system, you can assign a Secure Data Password and an Attendant Administrative Access Code.

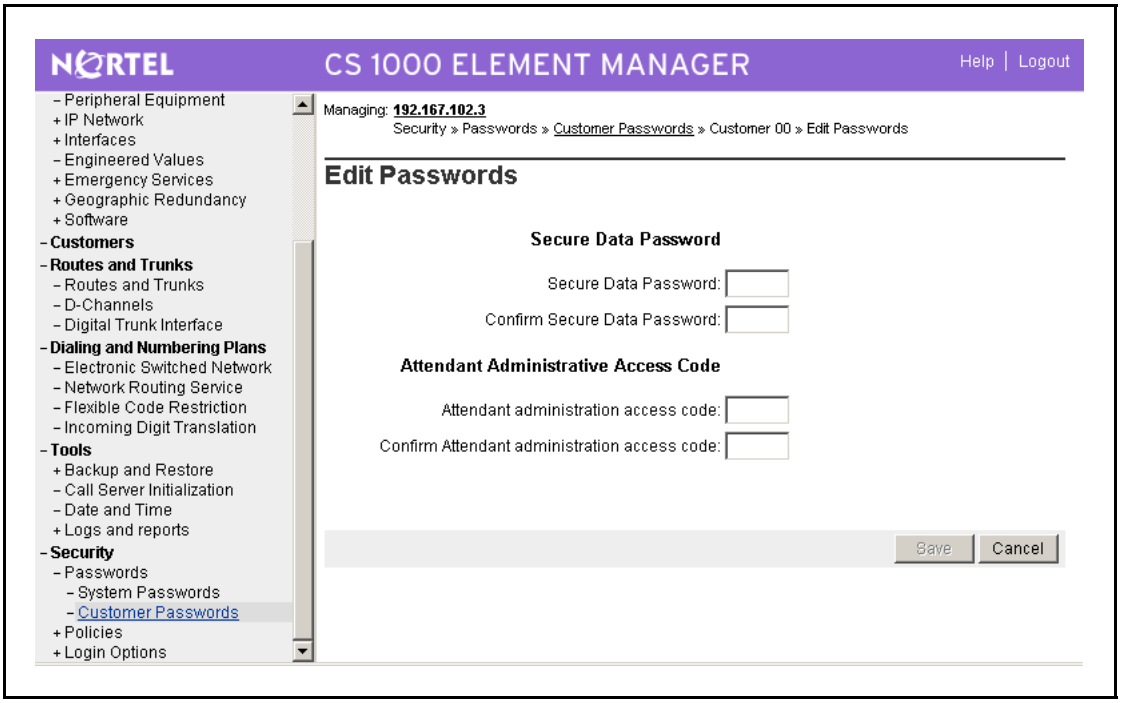
Use the following procedure to assign or change the Secure Data Password or Attendant Administrative Access Code.

Procedure 73
Assigning or changing customer passwords

Step	Action
1	Log on to Element Manager using a System password level 2 account.
2	Click **Security > Password > Customer Passwords** . The **Customer Passwords** page appears.



3	Click a Customer Number. The **Edit Passwords** page appears.



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 74
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 48
Variable definitions

Variable	Value
<account type>	The type of account to create.

Table 49
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 50 "Job aid: LD 17 user and password prompts" (page 233).

Table 50
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.
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 58 "Job aid: Password restrictions" (page 245).

Table 50
Job aid: LD 17 user and password prompts (cont'd.)

NEW_PASSWORD	a...a	New password. For password requirements, see Table 58 "Job aid: Password restrictions" (page 245).
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 75
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 53 "Job aid: Restrictions on LAPW user names and passwords" (page 237) 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 58 "Job aid: Password restrictions" (page 245) 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 51
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 76
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 53 "Job aid: Restrictions on LAPW user names and passwords" (page 237) 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 52
Variable definitions

Variable	Value
<customer num>	The customer number.
<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 53
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 77
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 54 "Example output from the PRT PWD command" (page 238) shows an example of the output from the PRT PWD command.

Table 54
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
```

Table 54
Example output from the PRT PWD command (cont'd.)

```
        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 78
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 55 "IPWD output" (page 240) shows an example of the output form the PRT IPWD command.

Table 55
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 79
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 50 "Job aid: LD 17 user and password prompts" (page 233).
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 56
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 80
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 81
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 50 "Job aid: LD 17 user and password prompts" (page 233).

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 82
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 83
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 282).

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 42). For recommendations about what password settings to use, see "Recommended password management practices" (page 18).

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 84
Configuring password settings 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**. You can bypass any of the following prompts by pressing **Enter**. For more information about the sequence of prompts for LD 17, see Table 50 "Job aid: LD 17 user and password prompts" (page 233).
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 58 "Job aid: Password restrictions" (page 245).
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 57
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 58
Job aid: Password restrictions

Password must be at least eight characters in length
The following characters are permitted: 0-9, A-Z, a-z, !$%^&()_- +={}|\:;"'<,>.?/
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. 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 85
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 282).

--End--

Table 59
Variable definitions

Variable	Value
<user name>	A PWD2 level user name.

Use the following procedure to reset the password on an MGC.

Procedure 86
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 60 "Password reset for other system devices and applications" (page 248).

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 60
Password reset for other system devices and applications

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	*IP Line Fundamentals (NN43100-500)* ()
Signaling Server	*Signaling Server Installation and Commissioning (NN43001-312)* ()

Multi-user login configuration using overlays

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

The Single Terminal Access (STA) feature 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 61 "User administration commands" (page 251).

Table 61
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

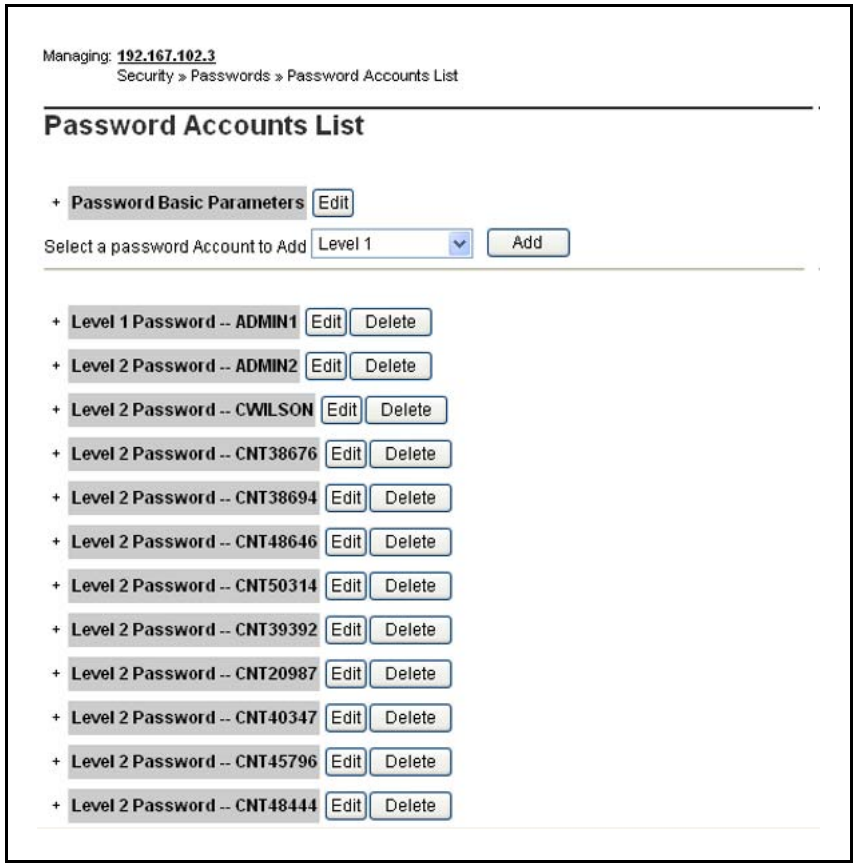
Use the procedures in this section to manage users, change passwords, and configure access restrictions using Element Manager. Users without the Administer Accounts privilege can change their own password only.

Add a user

Use the following two procedures to add user accounts.

Procedure 87
Adding a user other than LAPW by using Element Manager

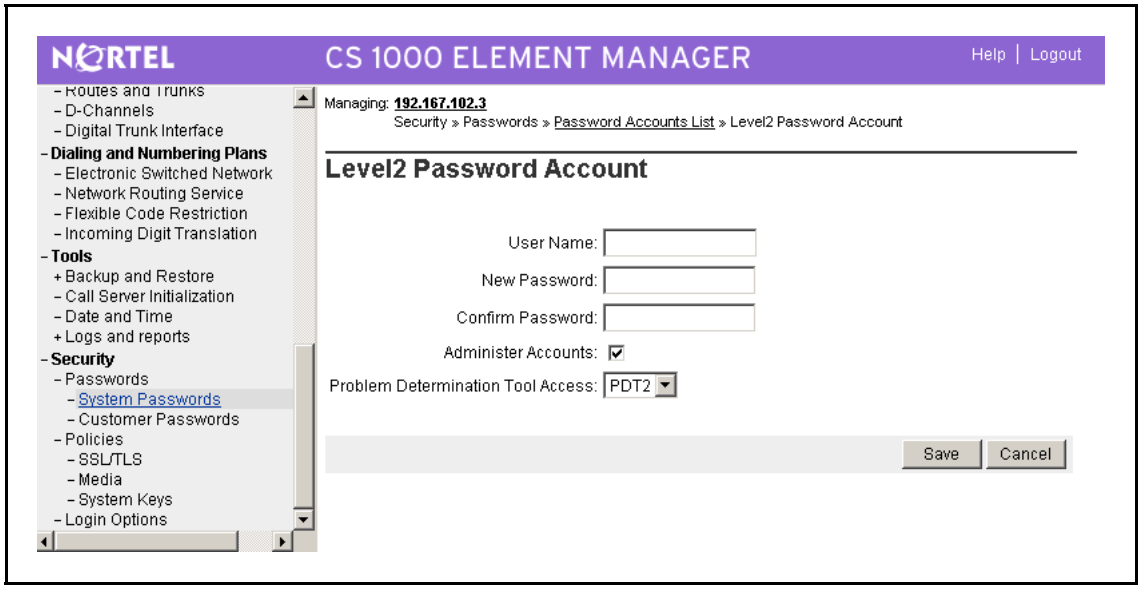
Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



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 39).

4 Click **Add**.

The **Password Account** page appears. The page varies slightly depending on what type of account you selected.



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.

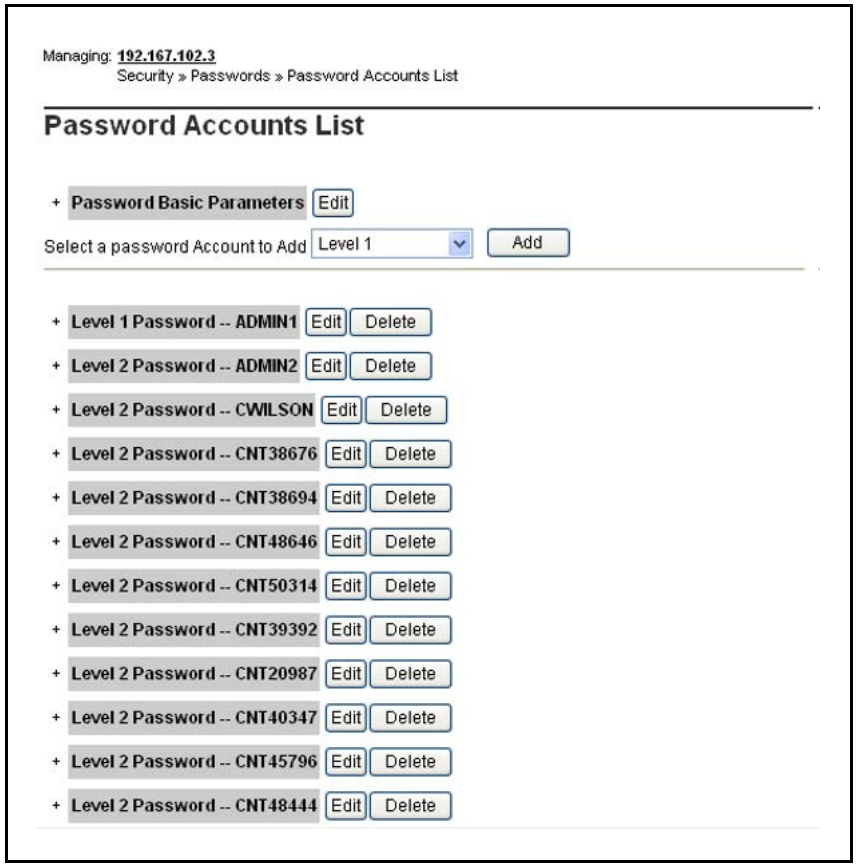
b If you are adding a Level 2 account, select or clear the **Administer Accounts** check box.

7 Click **Save** to save the new user, and return to the **Password Accounts List** page.

--End--

Procedure 88
Adding an LAPW user by using Element Manager

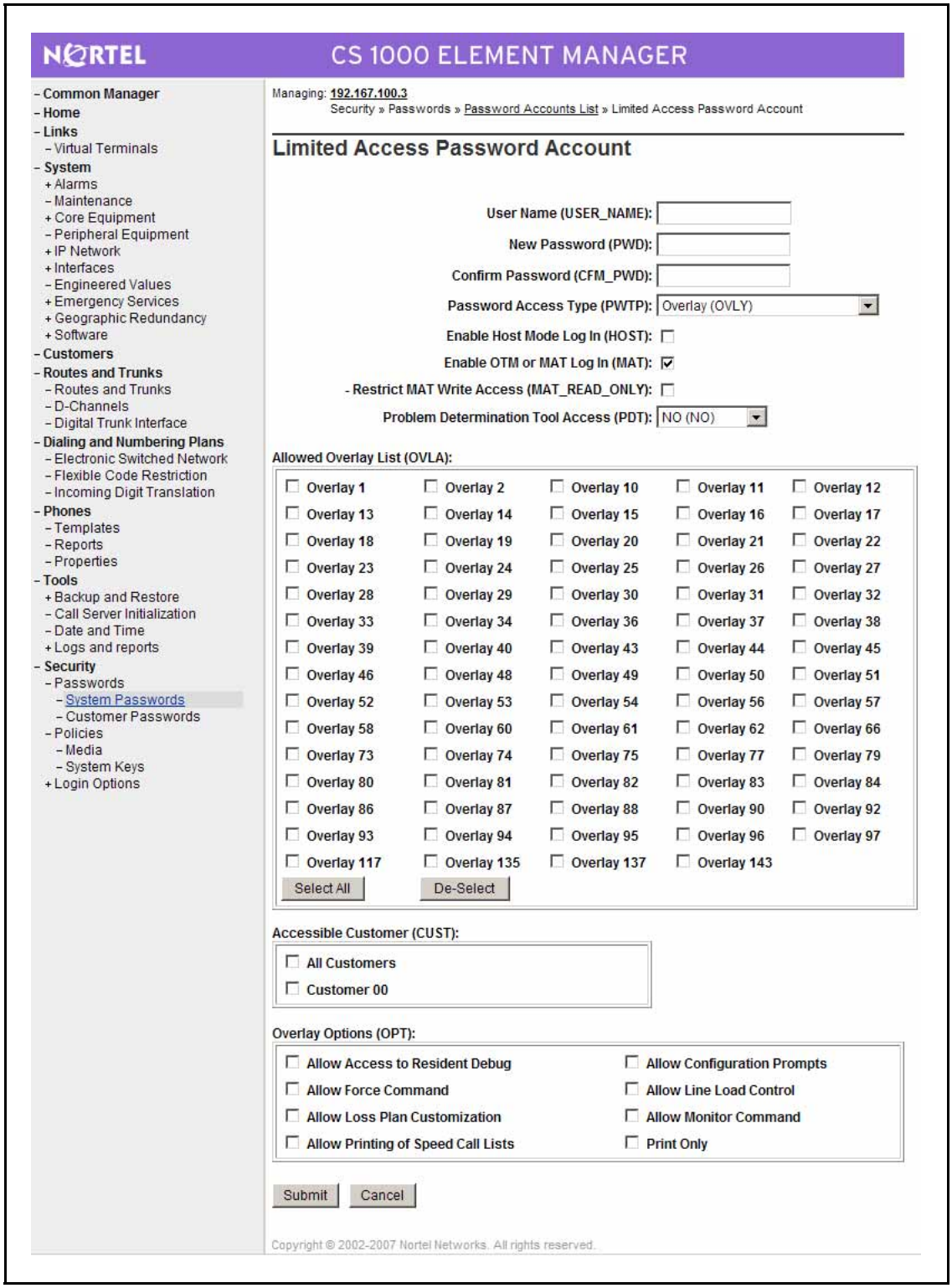
Step	Action
1	Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears.



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 39).

4 Click **Add**.

The **Limited Access Password Account** page appears.



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--

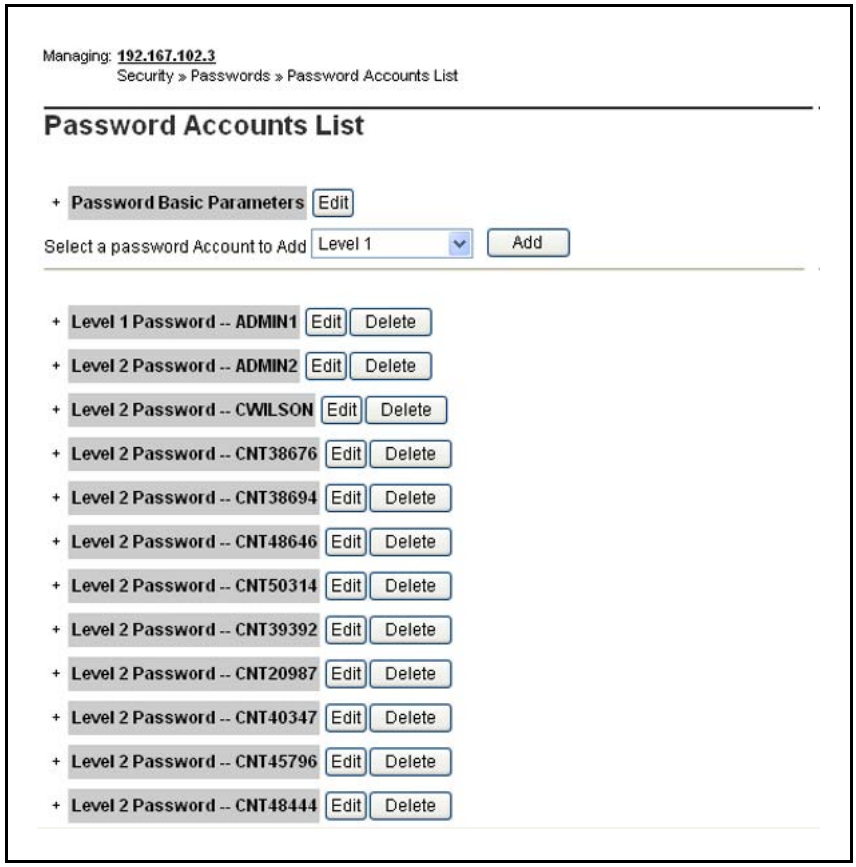
Edit an existing user

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.

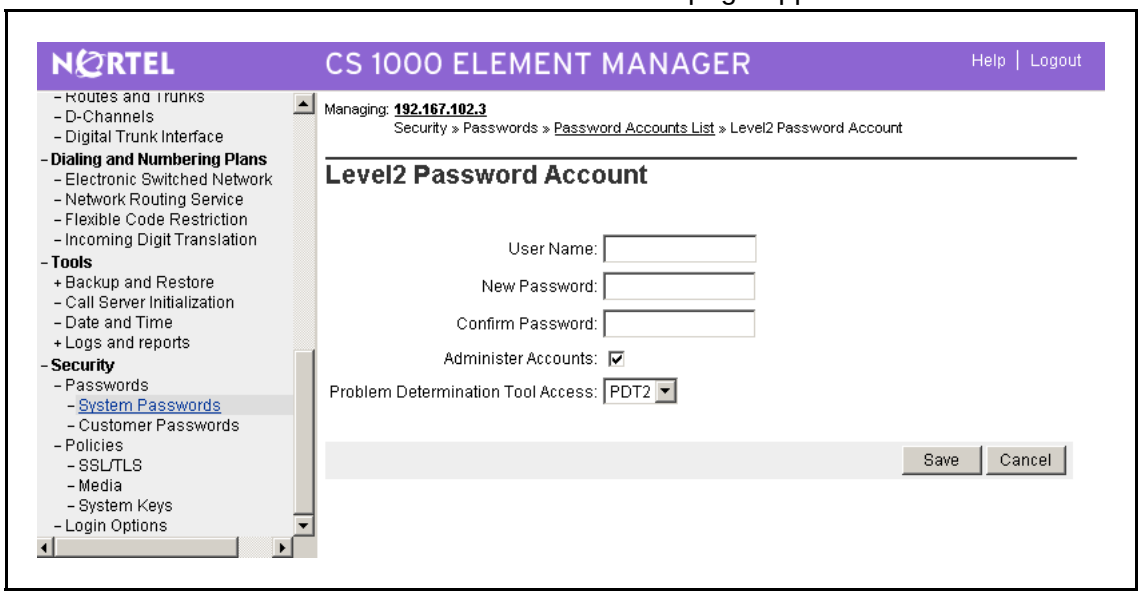
Procedure 89
Editing an existing user by using Element Manager

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.



3 Next to the account you want to modify, click **Edit**.

The **Password Account** page appears.



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 62 "Job aid: user and password management commands on the stand-alone NRS" (page 258).

Procedure 90
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 62
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.

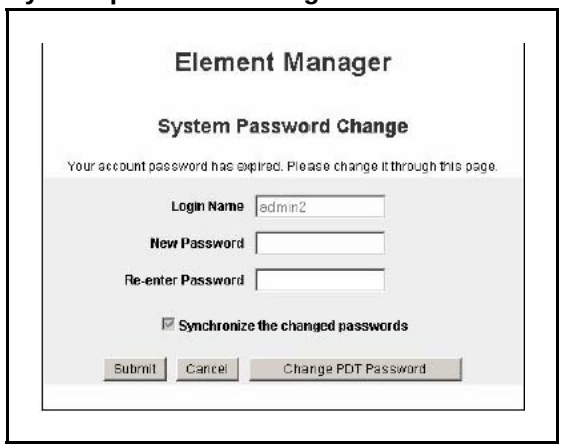
Table 62
Job aid: user and password management commands on the stand-alone NRS (cont'd.)

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 5 "System password change" (page 259).

Figure 5
System password change



Edit global password settings

Use the following procedure to configure settings that apply to all accounts.

Table 63
Job aid: password options

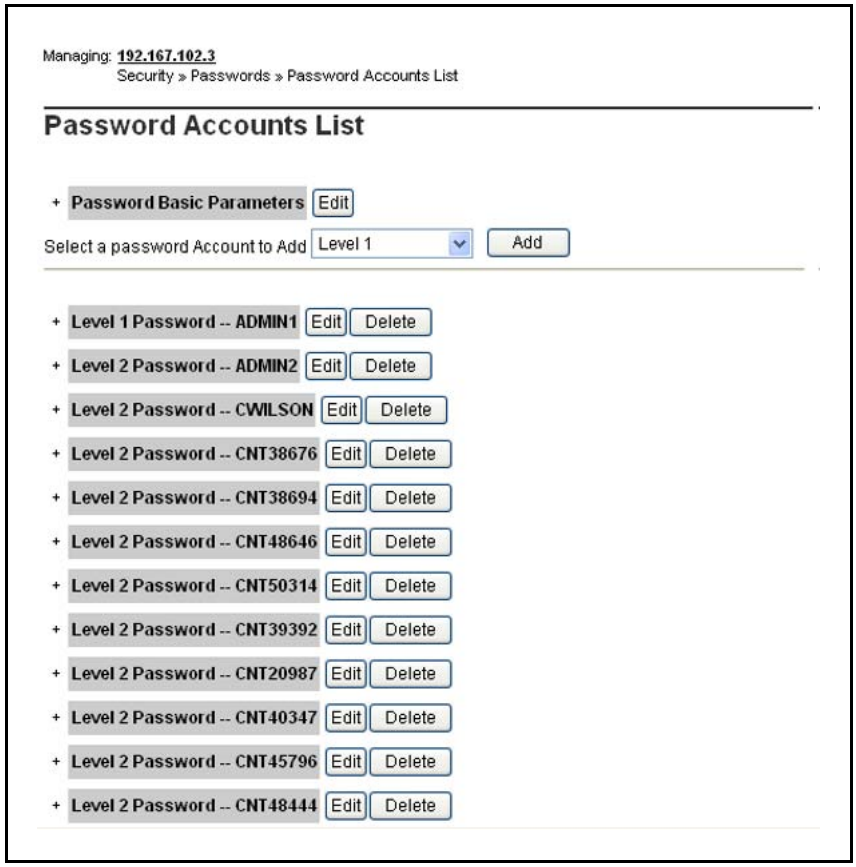
Password option	Effect
Force Password Change (FPC)	Prevents users from continuing to use the system default passwords.
Failed Log In Threshold	Controls the number of times a user can fail to log on before the port they are using is locked. To override a lockout, manually restart the system.

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 42).

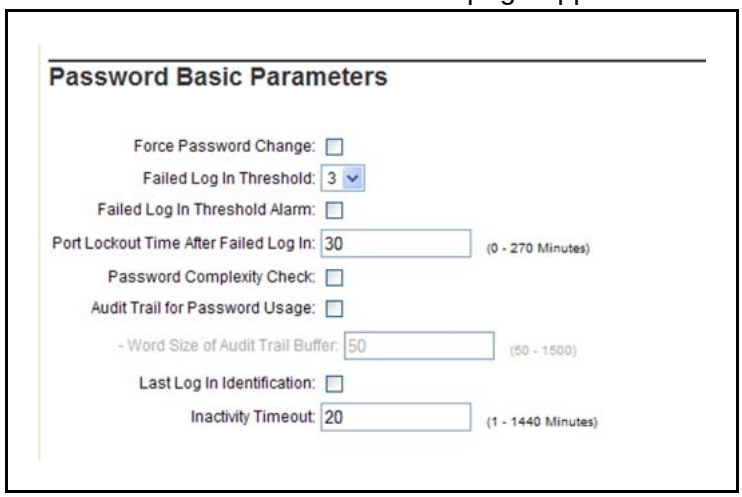
Procedure 91
Editing global password settings by using Element Manager

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.



3 Next to **Password Basic Parameters**, click **Edit**.

The **Password Basic Parameters** page appears.



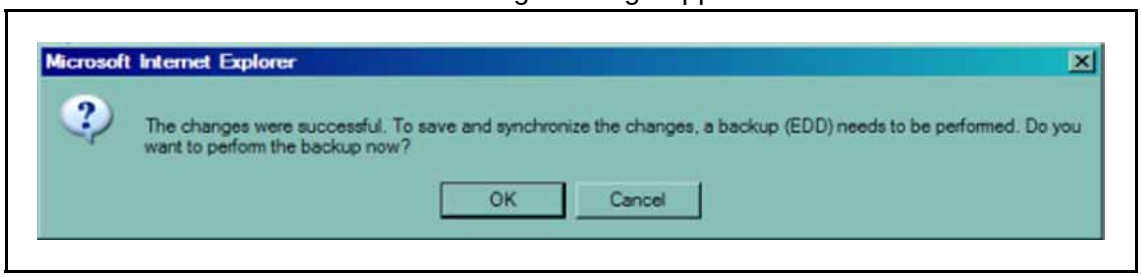
4 Edit any of the following parameters by selecting or clearing the check box, selecting from the list, or entering a value:

- 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:



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 259).

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

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 263))
- switchroom security (see "Switchroom security" (page 264))
- network facilities security (see "Network facilities security" (page 264))

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 242).

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.

Refresh system keys

Several components of the Communication Server 1000 (CS 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 64 "System keys that must be manually refreshed" (page 266).

Table 64
System keys that must be manually refreshed

Key	For more information see:
SSH	"Manage SSH keys using overlays" (page 272) or "SSH key management using Element Manager" (page 277)
ISSS	"Other ISSS configuration and maintenance procedures" (page 96)
TLS	SIP TLS can use the same key as Element Manager. See *Element Manager System Reference — Administration (NN43001-632)* ()
Web SSL (HTTPS)	*Element Manager System Reference — Administration (NN43001-632)* ()
N-Way redundancy	*Network Routing Service Installation and Commissioning (NN43001-564)* ()

When you refresh the SSH keys, SSH is unavailable until the new keys are generated. On most systems, this takes two to three minutes. However, on TDM-only systems that use SSC as the call processor it can take up to two hours.

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 18).

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 65 "Job aid: shell management commands in LD 117" (page 268).

Table 65
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 65 "Job aid: shell management commands in LD 117" (page 268).

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 66 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 269).

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 66 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 269).

--End--

Table 66
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.

Table 66
Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices (cont'd.)

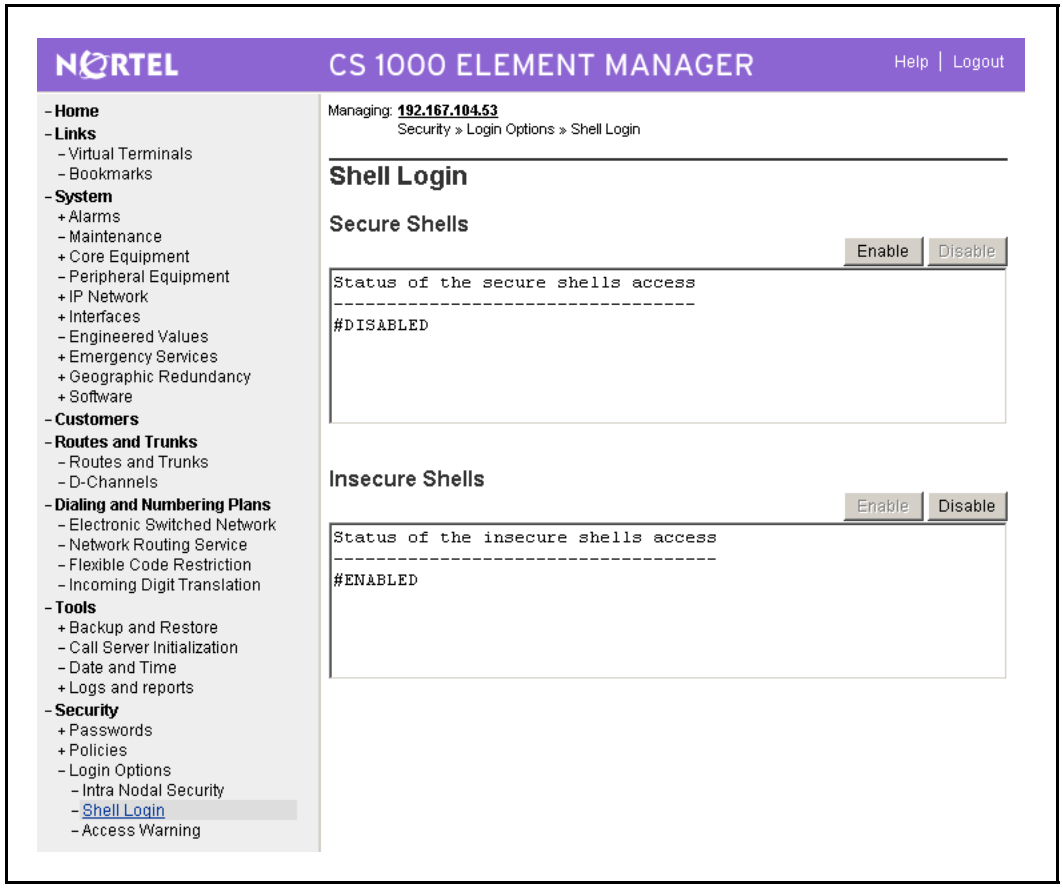
Command	Description
enlInsecureShells	Use this command to enable all insecure shells in the system. This includes Telnet and rlogin sessions.
statInsecureShells	Use this command to display the status of the insecure shell access.

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.



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 4 sessions on Small System Controller (SSC), or 16 sessions on a large 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 67
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.

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 68 "Job aid: arguments for SSH KEY GENERATE" (page 273).

The generated key is stored in a pending state until it is activated.

--End--

Table 68
Job aid: arguments for SSH KEY GENERATE

Command argument	Purpose
`SSH KEY GENERATE`	To generate a key on a one-CPU system.
`SSH KEY GENERATE ACTIVE`	To generate a key using the active core on a two-CPU system.
`SSH KEY GENERATE INACTIVE`	To generate a key using the inactive core on a two-CPU system.
`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 69 "Job aid: arguments for SSH KEY ACTIVATE" (page 273).

--End--

Table 69
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.

Table 69
Job aid: arguments for SSH KEY ACTIVATE (cont'd.)

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 70 "Job aid: arguments for SSH KEY SHOW" (page 274).

--End--

Table 70
Job aid: arguments for SSH KEY SHOW

Command argument	Purpose
SSH KEY SHOW	To display the fingerprint of the public key of the system.
SSH KEY SHOW ACTIVE	To display the fingerprint of the public key of the active core on a two-CPU system.
SSH KEY SHOW INACTIVE	To display the fingerprint of the public key of the inactive core on a two-CPU system.
SSH KEY SHOW CABINET [n]	To display the fingerprint of the public key of the expansion cabinet or MG1000E system. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

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 267).

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 71 "Job aid: arguments for SSH KEY CLEAR" (page 275).

--End--

Table 71
Job aid: arguments for SSH KEY CLEAR

Command argument	Purpose
SSH KEY CLEAR	To clear all of the public keys (active as well as pending) stored on the system.
SSH KEY CLEAR ACTIVE	To clear all of the public keys (active as well as pending) stored on the active core.
SSH KEY CLEAR INACTIVE	To clear all of the public keys (active as well as pending) stored on the inactive core.
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, activate, 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 **sshKeyGenerate** to generate the key on the Call Server, Media Gateway Controller (MGC), Signaling Server, or Voice Gateway Media Card. The generated key is stored in a pending state until it is activated.

--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, Signaling Server, 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 **sshKeyShow** to display the fingerprint of the public key of the Call Server, MGC, Signaling Server, 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 **`sshKeyClear`** to clear all of the public keys (active as well as pending) stored on the Call Server, MGC, Signaling Server, or Voice Gateway Media Card.

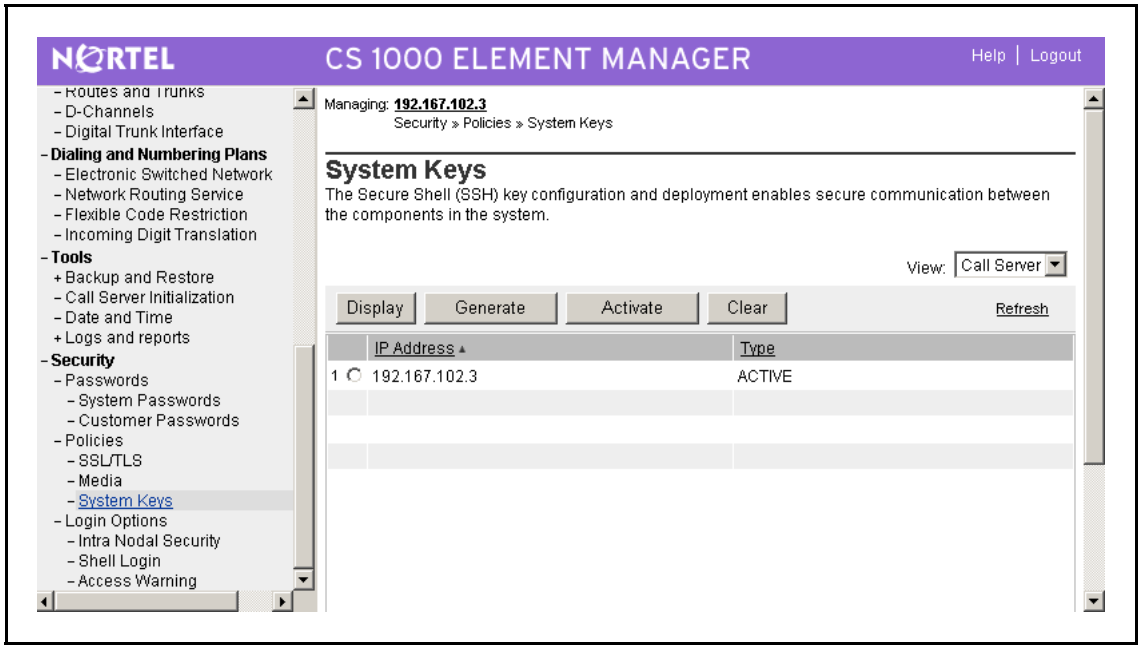
--End--

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), Signaling Server 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.



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 option 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 282).

Use the following procedure to restore the default text to the logon banner. Table 15 "Default text of the customizable logon banner" (page 44) 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--

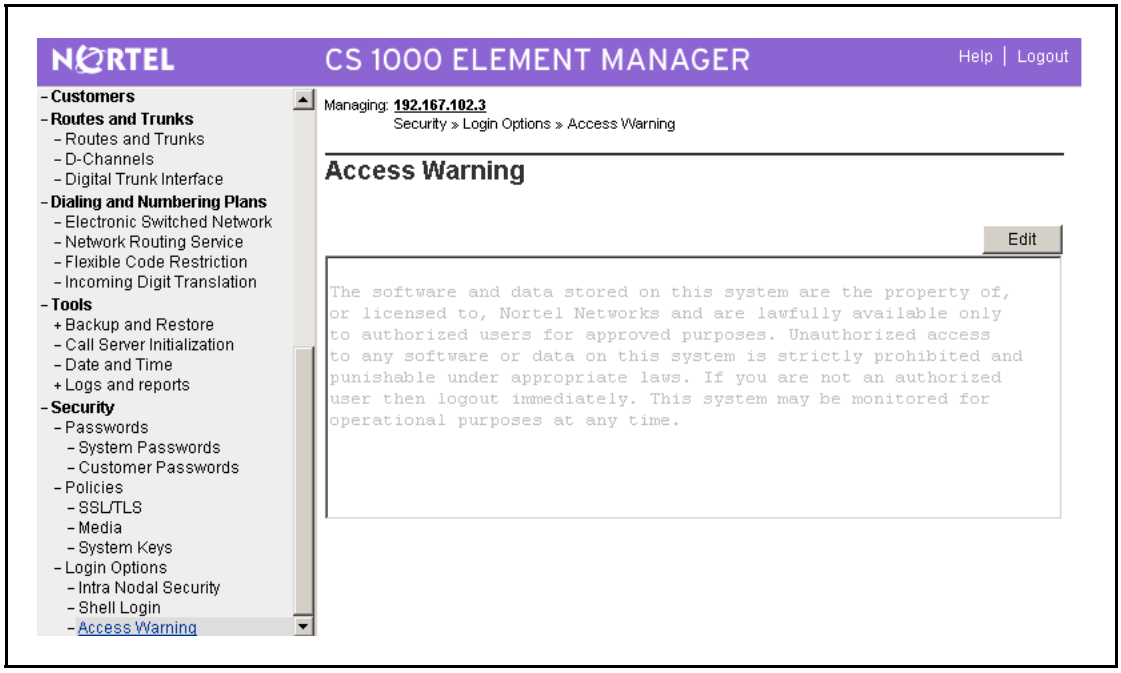
These changes are distributed to all Voice Gateway Media Card, MGC and IPMG devices the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see “Force an EDD using overlays” (page 282).

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.



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.

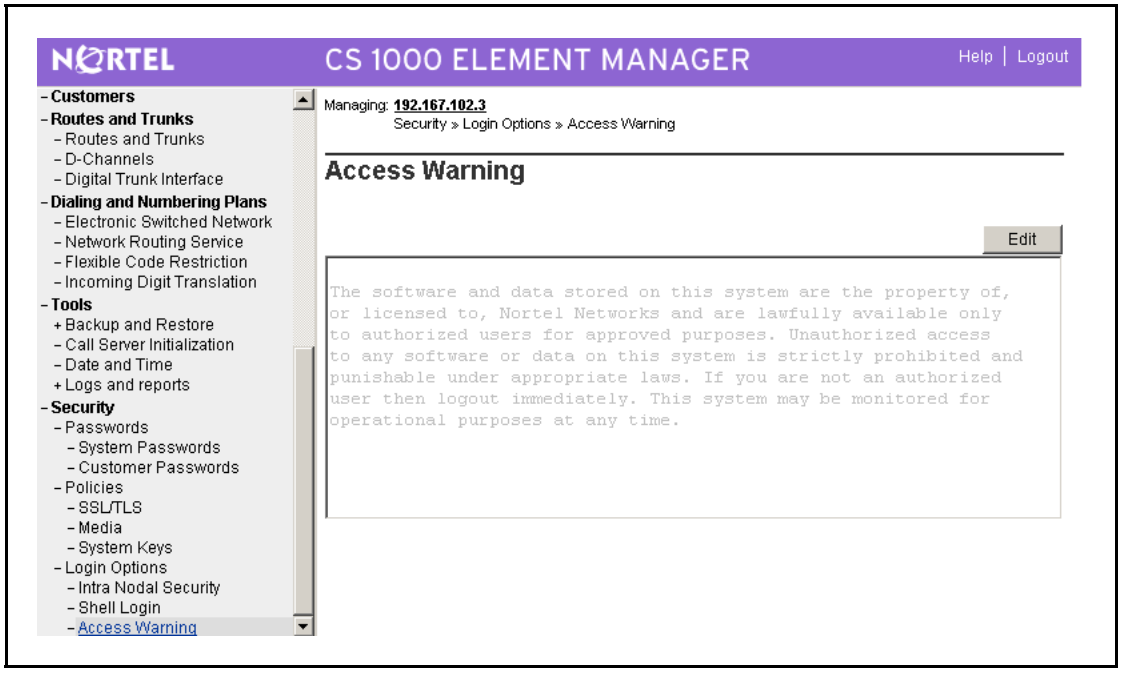
6 Click **OK** to save and distribute the banner file.

--End--

Use the following procedure to restore the default text to the logon banner. Table 15 "Default text of the customizable logon banner" (page 44) 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.



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 (CS 1000) system.

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 CS 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 112 “Decommissioning IPsec locally by using CLI” (page 285)

Use the following procedure to decommission IPsec locally on a Voice Gateway Media Card, Media Gateway Controller, or Signaling Server.

Procedure 112
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 113
Viewing IPsec profile 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 **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**.

Procedure 114
Confirming IPsec system settings on the active call server by using CLI or LD 117

Step	Action
1	Log on to the call server CLI.

2	At the LD 117 prompt, enter **CONFIRM ISEC**
	.
	The salt value, hashed IPsec PSK, system security status and system level appear, as shown in the following example:
	`>ld 117`
	`OAM000`
	`=> confirm isec`
	`Salt Value Hashed PSK Security Status Security Level`
	`----------`
	`4efc747d 35A1534CBD01B7BB575018C7A7BABAA6 Enabled Full Security`

3	Record the information reported by the CONFIRM ISEC command.
4	Log on to the OAM, PDT, or IPL CLI of the device for which you want to compare the IPsec configuration.

5 Enter **isecConfirm <salt value>**, where <salt value> is the salt value returned by the CONFIRM ISEC command at the LD 117 prompt.

The hashed IPsec PSK, system security status, and system level appear, as shown in the following example:

```
pdt> isecConfirm 4efc747d
Salt Value Hashed PSK Security Status Security
Level
-----------------------------------------------
-----------------------------
4efc747d 35A1534CBD01B7BB575018C7A7BABAA6 Enabled
Full Security
```

6 Compare the PSK, Security Status, and Security Level of the device with the values reported for the call server. If they do not match, see the procedures in "ISSS" (page 45) for more information about configuring ISSS.

--End--

Use the following procedure to view connection information for IPsec.

Procedure 115
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 116
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--

Use the following procedure to view information about IPsec configuration.

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 117
Viewing IPsec configuration by using LD 117

Step	Action
1	Log on to the call server CLI.
2	At the LD 117 prompt, enter either: **`prt ISEC {all | excep | target | sync}`** **OR** **`prt isectar`** Information about the targets, and about security status and level, both current and pending, appears.

--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 (CS 1000) Release 5.0 or 5.5.

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

Use the information in this section to access Media Security OMs.

Traffic measurement

Security enhancements introduced in CS 1000 Release 5.0 provide new traffic measurements as part of the IP Traffic Report (report 16), which is used to track progress of calls that use Media Security. The following 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 290).

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 290)

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
```

Multi-user login History file

The History File includes a separate Log File for each configured TTY port; this file records each technician's maintenance and administration activities. For more information about this file, see *System Management Reference (NN43001-600)* () .

TLS logs and alarms

Table 74 "SIP TLS OMs" (page 291) 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 292) 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

Appendix A: Standards

This appendix provides information about the Communication Server 1000 (CS 1000) system compliance with various security standards. The appendix is divided into the following sections:

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 76 "Encryption technologies used in CS 1000" (page 296) lists encryption technologies used in CS 1000 Release 5.0 and later.

Table 76
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.

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 CS 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 CS 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.

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.

SSC

Small System Controller.

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

I

K

L

M

N

P

R

S

T

U

V

Nortel Communication Server 1000

Security Management Fundamentals

Release: 5.5
Publication: NN43001-604
Document revision: 02.09
Document release date: 8 January 2009

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

www.nortel.com
LEGAL NOTICE

Sourced in Canada