Nortel Communication Server 1000

Security Management Fundamentals

NN43001-604

Document status: Standard
Document version: 01.05
Document date: 30 May 2007

Sourced in Canada

Revision history

May 2007
Standard 01.05. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.0 This document contains changes to SIP TLS configuration that rectify issues identified in CR Q01619113, and corrections to statements about password conversion identified in CR Q01620514.

May 2007
Standard 01.04. This document is up-issued to support CS 1000 Release 5.0 This document contains changes to SIP TLS configuration that rectify issues identified in CR Q01619113 and CR Q01617218.

May 2007
Standard 01.03. This document is up-issued to support CS 1000 Release 5.0 This document contains changes to Media Security configuration that rectify issues identified in CR Q01598513.

May 2007
Standard 01.02. This document is up-issued to support CS 1000 Release 5.0 This document contains changes to NKEY configuration ranges that rectify issues identified in CR Q01606037.

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

Contents

New in this release

Security Management Fundamentals (NN43001-604) is a new document that provides information about security features in CS 1000, and provides information about IP security features, as well as information about operations, administration, and maintenance (OAM) features.

The following sections detail what's new in *Security Management Fundamentals (NN43001-604)* for Communication Server 1000 (CS 1000) Release 5.0:

- "New security features in CS 1000 Release 5.0" (page 13)
- "Other changes" (page 14)

New security features in CS 1000 Release 5.0

CS 1000 Release 5.0 offers improvements to existing security features. It also introduces new features that protect the system against intrusion or misuse, and that protect information transmitted within or between systems.

The following enhancements improve OAM security:

- enhanced account management
- security event logging operations
- remote shell access controls
- secure remote shell access
- customizable logon banner

The following security features are new in CS 1000 Release 5.0:

- Secure remote access is provided by Secure Shell (SSH).
- Security for individual call streams is provided by the Media Security feature.
- Security for ELAN subnets is provided by an Intrasystem Signalling Security (ISSS) solution based on the industry standard IP Security (IPsec).
- Security for SIP signaling is provided by Transport Layer Security (TLS).

- Security for data exchanges between the IP Phones and the Signaling Server is provided by Secure UNIStim signaling, which requires a Secure Multimedia Controller (SMC) 2450 device.

All of these enhancements work in conjunction with existing security features to provide a more complete security solution.

Other changes

This section describes changes to this document other than those mandated by new security features.

Document restructuring and renaming

In CS 1000 release 4.5 and earlier, *System Security Management (553-3001-302)* contained security information. In CS 1000 Release 5.0, the two documents described in Table 1 "New security documents" (page 14) contain security information.

Table 1
New security documents

Access Control Management Reference (NN43001-602)	Describes how to limit access to calling features.
Security Management Fundamentals (NN43001-604) (This document)	Describes how to protect the system, including how to configure IP security, how to manage security certificates, and how to manage users and passwords.

The majority of the material formerly in *System Security Management (553-3001-302)* is now in *Access Control Management Reference (NN43001-602)*, except sections pertaining to OAM security are now in *Security Management Fundamentals (NN43001-604)*.

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 *Access Control Management Reference (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 18).

Table 2
Other NTPs that contain security information

Access Control Management Reference (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)

About this document

This chapter 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.

Intended audience

This document is intended for administrators responsible for configuring security features.

Subject

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 5.0 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:

- CS 1000E CP PII
- CS 1000E CP PIV
- CS 1000E CPPM HA (Chassis)
- CS 1000E CPPM HA (AC Cabinet)
- CS 1000E CPPM HA (DC Cabinet)
- CS 1000E CPPM SA (Chassis)
- CS 1000E CPPM SA (AC Cabinet)
- CS 1000E CPPM SA (DC Cabinet)
- CS 1000M Multi Group CP PIV Base Pkg (AC)
- CS 1000M Multi Group CP PIV Base Pkg (DC)
- CS 1000M Single Group CP PIV Base Pkg (AC)
- CS 1000M Single Group CP PIV Base Pkg (DC)

Applicable system components

This document applies to the following system components:

- Media Gateway 1000E Chassis
- Media Gateway 1000E Chassis Expander
- Media Gateway 1000E Cabinet
- Media Gateway 1000E Expansion
- Media Gateway 1000B CP PM

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

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
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

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 31)

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 149))
- program access control (see *Access Control Management Reference (NN43001-602)*)
- Audit Trail review (see "Configure LAPW Audit Trail using overlays" (page 158))
- History File review (see "History File configuration using overlays" (page 167))

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.
- Enable Default Password Change to prevent the use of system default passwords.
- Enable Password Complexity Check to prevent users from choosing simple passwords.
- Enable Failed Log In Threshold and configure it to permit three attempts.

Upgrading user names from an earlier release

The following OAM security issues pertain to upgrading to Communication Server 1000 (CS 1000) Release 5.0 from a previous release:

- 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 3 "User names created when accounts without user names are converted from CS 1000 Release 3.0" (page 22).
- Users are required to choose a new password the first time they log in after the system is upgraded. This occurs because system passwords are not converted upon system upgrade. For more information, see "System upgrade password conversion" (page 42).

Table 3
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 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 (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 recommendations

Protect Embedded Local Area Network (ELAN) messages by enabling ISSS with at least the minimum setting (Optimized Security). ISSS is particularly important if IP Phones are part of the system.

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). SIP security is important if IP Phones are part of your system. 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 over SIP trunks using key management protocols 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

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 except as needed. For instance:

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

Security certificates

You can configure the CS 1000 system to work with certificates provided by a common third-party certificate authority (CA), such as the Nortel Enterprise Common Manager (ECM), or with certificates that are self-signed. Nortel recommends that you implement the common third-party CA, because this option provides highly reliable security.

If the CA is not available, users 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

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. 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.

Upgrading from an earlier release

The following security administration issues pertain to upgrading to CS 1000 Release 5.0 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 to CS 1000 Release 5.0, new key pairs are generated for this certificate, and are used for both TLS and HTTPS.
- When you upgrade a SIP Gateway System from CS 1000 Release 4.5 to CS 1000 Release 5.0, the steps to install third-party CA-signed certificates vary depending on whether you request and install the certificate before upgrading, or after upgrading the system.
  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 not yet upgraded the system, Nortel recommends that you carry out the steps in Procedure 28 "Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading" (page 109), and Procedure 29 "Processing a pending certificate response for SIP TLS when upgrading" (page 113), before you perform the system upgrade.

Security interactions

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

ISSS and Element Manager over ELAN

If you configure ISSS to Full Security, you must enable SSL/TLS on Element Manager, or Element Manager cannot operate over the ELAN subnet. For an overview of the interaction of ISSS with Element Manager, see Table 4 "Interactions between ISSS and Element Manager over ELAN" (page 25).

Table 4
Interactions between ISSS and Element Manager over ELAN

ISSS configuration option	Element Manager operation
Full Security	Element Manager can operate over the ELAN subnet only if SSL is enabled.
Functional Security, Optimized Security, No Security	Element Manager operates normally, regardless of SSL configuration.

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

ISSS and ECM with Element Manager

If you are using Element Manager under ECM to manage the system, Nortel recommends that you enable ISSS to protect confidentiality of communication between Element Manager and the system.

Configure each Element Manager managed by ECM to use the same secret. Nortel recommends changing the secret manually every few months. For more information about secrets that you must refresh manually, see "Refresh system keys" (page 183).

ISSS and Geographic Redundancy

If the system is configured to use ISSS at the FULL level, ISSS can prevent the Geographic Redundancy feature from using FTP. The Geographic Redundancy feature uses FTP to transfer customer configuration data from the Primary Call Server to the Secondary or Alternate Call Servers. Therefore, if you configure the system to use both Geographic Redundancy and ISSS configured to FULL, Nortel recommends that you edit the IPsec target list on each call server. 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.

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, all links among all known elements are encrypted, except SSH, Network Time Protocol, and Applications Module Link (AML). Both SSH and Network Time Protocol have their own encryption, so ISSS is not required to protect them. AML does not have its own encryption, but 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 57 "Adding an ISSS target manually by using Element Manager" (page 143).

Table 5 "Interactions between ISSS and AML" (page 26) shows specific interactions of devices that rely on AML.

Table 5
Interactions between ISSS and AML

Application or feature	Interaction
CallPilot	Operates normally when ISSS is enabled, but cannot take advantage of the encryption offered by ISSS unless you complete the following steps: • verify that the version of CallPilot running on your system supports ISSS

	• manually add the CallPilot IP address as an IPsec target You can configure CallPilot to use either Full or Functional setting levels. If you plan to use Enterprise Common Manager (ECM), configure CallPilot to use the Functional Security setting.
Symposium Call Center	Operates normally when ISSS is enabled, but cannot take advantage of the encryption offered by ISSS unless you complete the following steps: • verify that the version of Symposium Call Center running on your system supports ISSS • manually add the Symposium Call Center IP address as an IPsec target.
ECM for Element Manager	Operates normally when ISSS is enabled, but cannot take advantage of the encryption offered by ISSS unless you manually add the ECM IP address as an IPsec target. ECM can use ISSS only if all the managed systems use the same ISSS shared secret.

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

Some third-party SIP phones are unable to receive calls that offer Media Security. Therefore, 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, the third-party phones reject incoming calls from the IP Phones.

If your system has both third-party SIP phones and IP Phones capable of SRTP connections, and calls between them fail, Nortel recommends that you configure the IP Phones to have a Class of Service for Media Security of Never (MSNV).

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 Media Security for all connections cannot access CallPilot. For more information about the interaction of Media Security Class of Service with CallPilot access, see Table 6 "Interactions between Media Security and CallPilot on systems without MGC daughterboards or MC32S" (page 28).

Table 6
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) with MC32S cabinets.

SIP TLS security policy interaction with Failsafe NRS

The SIP TLS Secure End-to-End and Secure Local policy settings prevent the operation of Failsafe NRS. If you are configuring TLS on a system where you use, or plan to use, Failsafe NRS, Nortel recommends that you use Best Effort policy for TLS. If you require that all calls be encrypted, use Secure End-to-End policy, but be aware that this prevents Failsafe NRS from functioning. See Table 7 "Consequences of SIP trunk security" (page 28) for an explanation of the consequences of SIP TLS security configuration on Failsafe NRS.

Table 7
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, the firewall can interact with SIP TLS to prevent SIP trunks from communicating with the Signaling Server or SIP Proxy. To prevent the SMC 2450, or any firewall, from blocking SIP trunks that are protected by TLS, verify that the port that is configured for TLS is opened (the default port for TLS is 5061).

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:

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

Transport layer 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 insecure 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 45).

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 8 "IP Phones capable of establishing a secure connection using Media Security" (page 33).

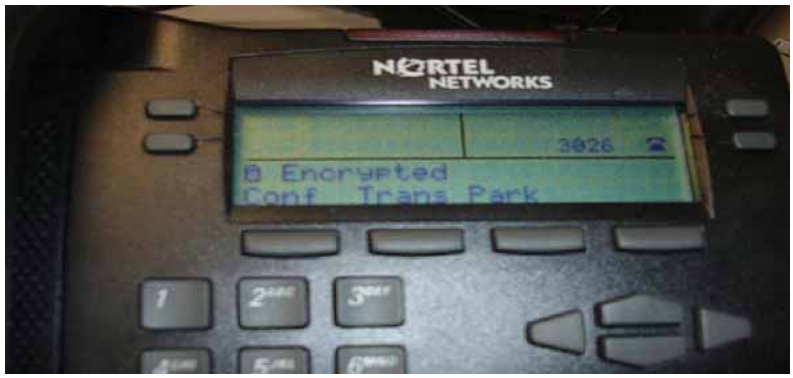
Table 8
IP Phones capable of establishing a secure connection using Media Security

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

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 33); 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 61).

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 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, Security Certificates, and NRS SIP Proxy.

IPsec

The IP Security framework (IPsec) provides an ISSS solution that works with all IP protocols. For procedures relating to ISSS, see "ISSS" (page 131).

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. Encryption is accomplished by configuring the endpoints to share a secret, and that secret is used as part of an encryption and decryption algorithm. The secret can take the form of a preshared key (PSK), or a key can be shared automatically using public key cryptography.

ISSS is disabled by default. If you want to use ISSS, you must configure it and restart the system. During startup, the system loads the following ISSS system profile information from the ISSS configuration files:

- PSK from psk.txt file
- ISSS security level and status from isec.txt
- target list from nodexxxx.cfg for pbxLink, ipmgConf.db for MGC, and config.ini for call server and nodes
- target list from target.txt file

The default ISSS status for each target is the same as the system ISSS status, unless you configure the target to have a different status. If you configure a target to have a specific status, 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 insecure 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. Therefore 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 must be exchanged in one of the following ways:

- exchanged individually between endpoints in the system. This method requires that the exchange 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 message containing a random session key, and the encrypted message 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, 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. This type of signature uses the IP address of the device sending the certificate, so it can provide reliable security in networks where the number of IP addresses is fairly small, making the owner's identity easy to verify.

— Certificates issued by a local private CA or a third-party CA use Public Key Infrastructure (PKI). The CA signs the certificates, thereby verifying the identity of the owner of the certificate.

For more information about security certificates, see "Security certificate concepts" (page 37).

Security certificate concepts

In security systems that rely on secret keys, keys must be securely exchanged. This is not always practical in large networks, so security certificates are used in conjunction with public-private key pairs. Certificates are digitally signed to verify the ownership of the public key contained in the certificate, and are widely used to protect communications on networks that support SSL encryption.

CS 1000 Release 5.0 can use certificates of any of the following types:

- generated and signed by the private CA on the Primary SIP Proxy system (NRS).
- generated and signed by common third-party CAs, such as Verisign, Thawte, or Entrust.
- generated and signed by the owner of the certificate (self-signed). Self-signed certificates are used for encryption only, and do not provide authentication of identity.

CS 1000 Release 5.0 uses certificates to protect two types of communication:

- Web SSL certificates for communication using HTTPS
- SIP TLS certificates for communication using SIP trunks

The SIP TLS implementation on CS 1000 Release 5.0 can use the same X.509 public-key certificate as Element Manager. The certificate is associated with each individual application on the Signaling Server.

You can use Web SSL to provide HTTPS signaling. To do so, you must assign a security certificate to each endpoint that you wish to protect using Web SSL, including system devices such as CS 1000 elements and Networking Routing Service (NRS). Similarly, to use TLS to protect SIP trunking, you must assign a certificate to each SIP endpoint.

To sign a certificate service request (CSR), a certificate authority must have its own root or intermediate certificate.

In the case of SIP TLS, for the client to verify a certificate received from the server, the certificate must be installed in the client Certificate Authorities list. Similarly, for the server to verify the a certificate received from the client, the certificate must be installed in the server Certificate Authorities list.

Private-CA certificates are automatically put into the Certificate Authorities list of the system that owns the certificate. However, you must install third-party and self-signed certificates using the Enterprise Common Manager (ECM) web interface.

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 third-party CA (the root) is reached. This sequence of verification is sometimes referred to as a chain of trust.

In CS 1000 Release 5.0, 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 9 "Examples of certificates in a chain" (page 38).

Table 9
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 SecurityAdministrator access.

For certificate and CA management procedures, see "Security certificates" (page 75).

NRS SIP Proxy

SIP Proxy mediates between trusted and nontrusted SIP endpoints. For more information about SIP Proxy, see *Network Routing Services 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 149).

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.

ATTENTION

To configure or access many security features, you must log on with an account that has SEC_ADMIN privilege. The SEC_ADMIN privilege is available to Level 2 (PWD2) user accounts that are configured with the authority to administer accounts.

System accounts

Default user names and passwords are available for each of two modes of operation in 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. For a description of the system accounts and passwords, see Table 10 "System accounts and passwords" (page 40).

Passwords are case-sensitive. You can use digits from 0 to 9 and alphabetic characters A through Z in passwords.

The OAM modes are:

- PWD Level 1 user ID and password (PWD1)
- PWD Level 2 user ID and password (PWD2)

The PDT modes are:

- PDT Level 1 user ID and password (PDT1)
- PDT Level 2 user ID and password (PDT2)

Table 10
System accounts and passwords

User	Passwords		
	Call server	Signaling Server	Voice Gateway media Card
ADMIN1: PWD1 (Level 1)	Default password (configured by the system)	Synchronized from the call server	Synchronized from the call server
ADMIN2: PWD2 (Level 2)	Default password (configured by the system)	Synchronized from the call server	Synchronized from the call server
PDT Level 1	Default password (configured by the system)	Not applicable	Not applicable
PDT Level 2	Default password (configured by the system)	Synchronized from the call server	Synchronized from the call server

User	Passwords		
	Call server	Signaling Server	Voice Gateway media Card
LAPW (Limited Access)	Default password (configured by the system)	Not applicable	Not applicable
IP Phone Installer Password	Not applicable	No default password	No default password

The call server Level 1 password (PWD1), Level 2 password (PWD2), and PDT Level 2 password (PDT2) become the system passwords 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 password (PWD1), Level 2 password (PWD2), and PDT Level 2 password (PDT2) accounts are described in Table 11 "Password level descriptions" (page 41).

Table 11
Password level descriptions

Password type	Description
Level 1 password	The administrator can use the Level 1 password to log on to the system to change the configuration database. Users that have Level 1 passwords cannot change Level 1 passwords, Level 2 passwords, or the secure data password associated with assigning Authorization Codes (Authcodes) and DISA parameters (if defined).
Level 2 password	The Level 2 password provides all privileges of the Level 1 password as well as the ability to administer accounts.
Limited Access Password (LAPW)	The Limited Access to Overlays feature can be configured to require a user name of up to 11 alphanumeric characters for LAPW accounts. The user name can be configured only by an administrator using the Level 2 password.

For more information about creating or changing passwords, see Table 22 "Job aid: LD 17 user and password prompts" (page 153). To print all accounts that have insecure passwords, see Procedure 74 "Checking for insecure passwords using LD 22" (page 167)

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 *Access Control Management Reference (NN43001-602)*.

System upgrade password conversion

In CS 1000 Release 5.0, all passwords are encrypted using SHA-256. The first time a user logs on after you upgrade the system to CS 1000 Release 5.0, the encryption for that user's password is converted to SHA-256.

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 following basic role 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.

For more information about role-management and other security features available in ECM, see *Enterprise Common Manager Fundamentals (NN43001-116)*.

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.

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 181).

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 SL1 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 12 "Default text of the customizable logon banner" (page 44).

Table 12
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.

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. 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 in CS 1000 Release 5.0, 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 13 "Configuration options available for Media Security" (page 46) shows the configuration possibilities for the Media Security feature.

Table 13
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	
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 14 "Details of Class of Service options for Media Security" (page 46).

Table 14
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 instance, 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 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 is capable of providing 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)*.

Procedure 1
Configuring system-wide Media Security using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 Media Security 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 Media Security 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 Media Security 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 **<n>** at the LD 17 NKEY prompt, where <n> is an integer in the range of 16-31.

The default value for <n> 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.

7 Enter **<value>** at the LD 17 TKEY prompt where <value> is 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.

—End—

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)*.

Procedure 2
Configuring Class of Service using LD 11

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 **YES** at the LD 11 ECHG prompt.
5	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.

—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 47). 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)*.

Procedure 3
Configuring VTRK Class of Service using LD 14

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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, enter **VTRK**. Entering any other VTRK value causes an error.

6 At the LD 14 CUST prompt, enter **0**.

7 At the LD 14 RTMB prompt, enter **xx**.

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 At the LD 14 TKID prompt, make no entry.

—End—

Media Security configuration using Element Manager

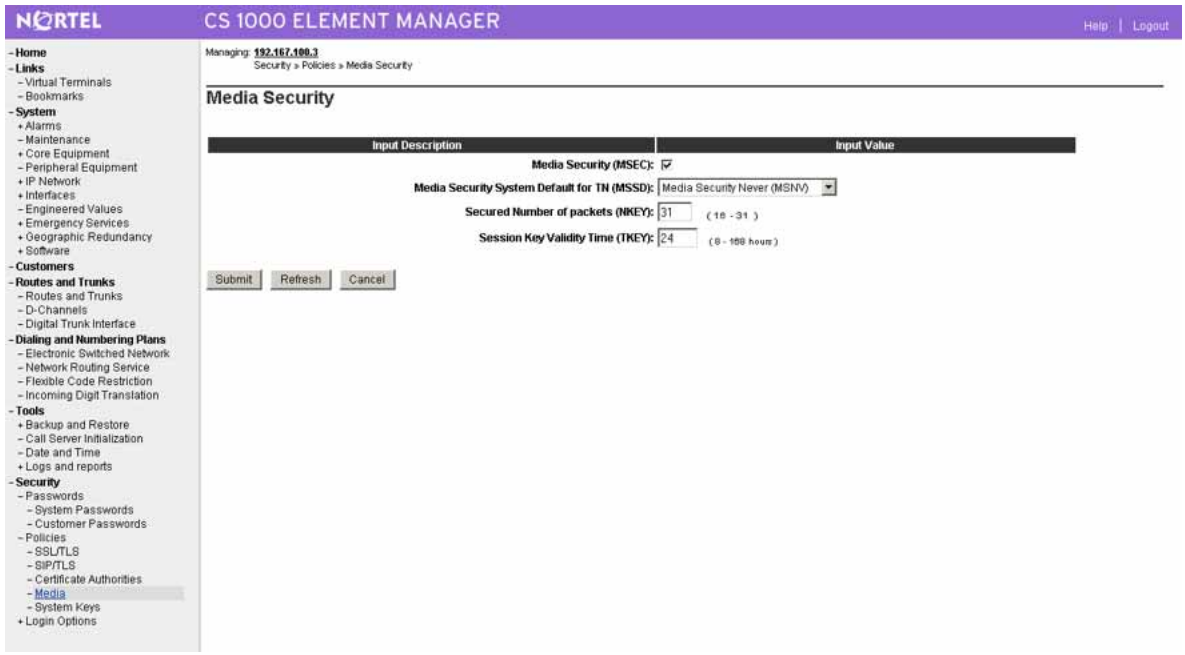
Use the procedures in this section to configure Media Security using Element Manager.

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 2 "Media Security configuration" (page 52). For more information about configuring Element Manager, see *Element Manager System Reference — Administration (NN43001-632)*.

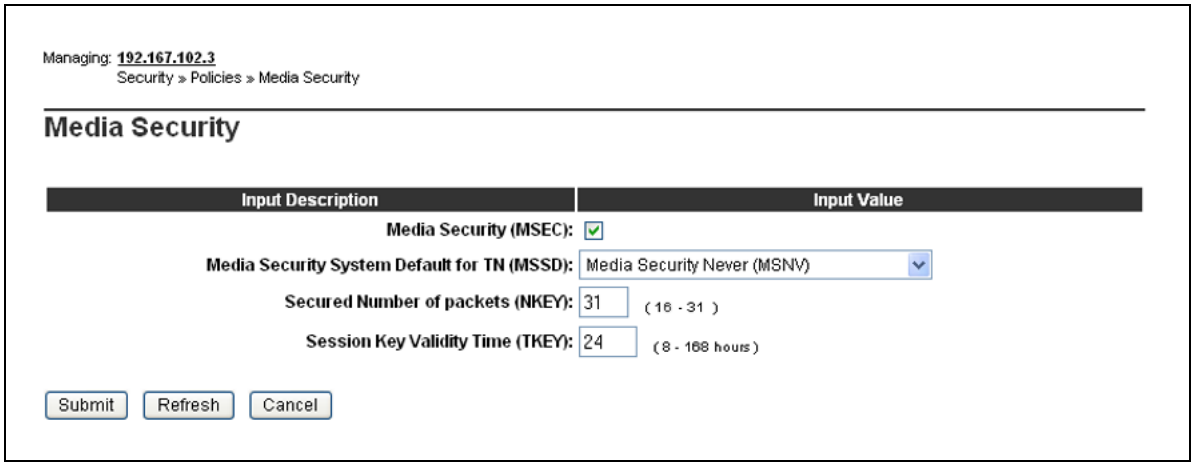
Figure 2
Media Security configuration



Procedure 4
Configuring system-wide Media Security using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Policies > Media** . The **Media Security** page appears, as shown in Figure 3 "Media Security " (page 53).

Figure 3
Media Security



3 Choose one of the following options:

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

OR

Clear the **Media Security** check box to disable 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.

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 Choose one of the following options:

Click **Submit** to save your changes.

OR

Click **Cancel** to discard your changes.

—End—

VTRK Class of Service configuration

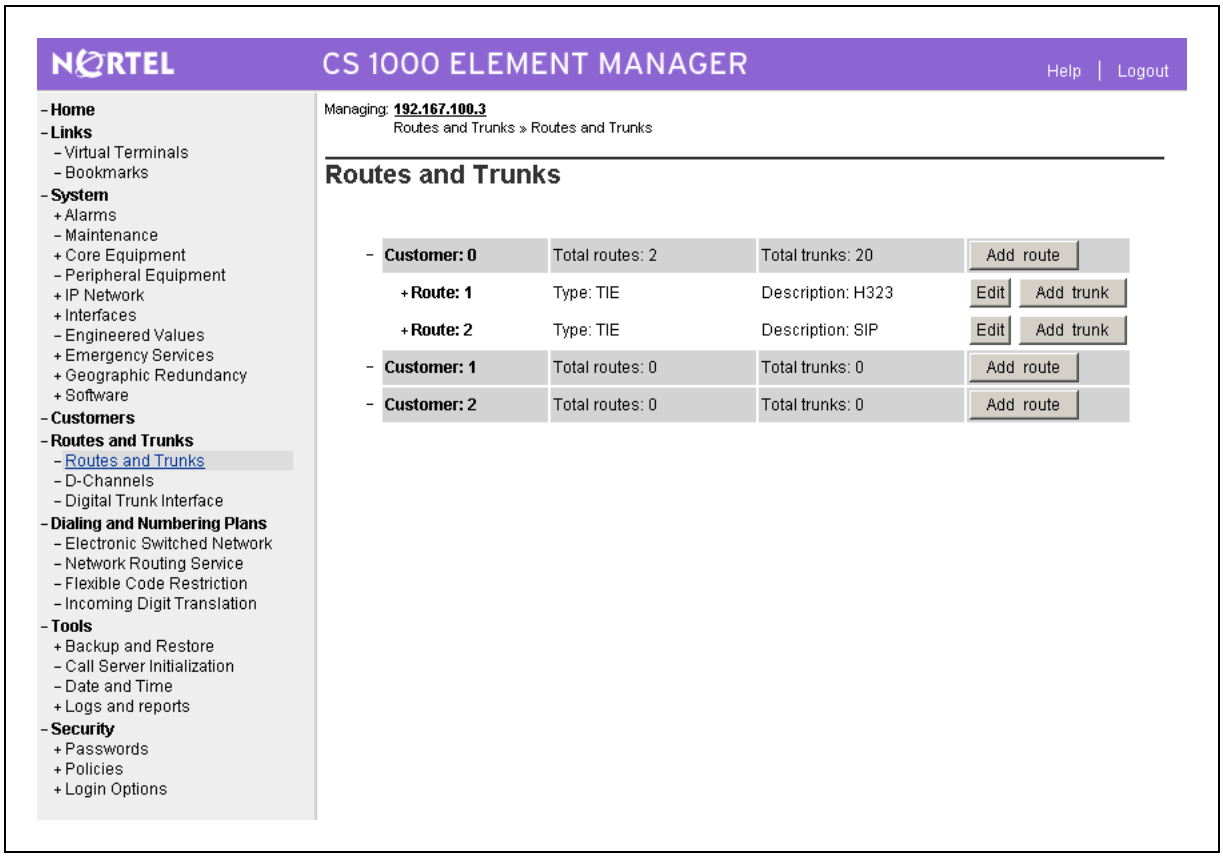
You can configure Media Security Class of Service for Virtual Trunks (trunks that have XTRK configured as VTRK).

Procedure 5

Configuring VTRK Class of Service using Element Manager

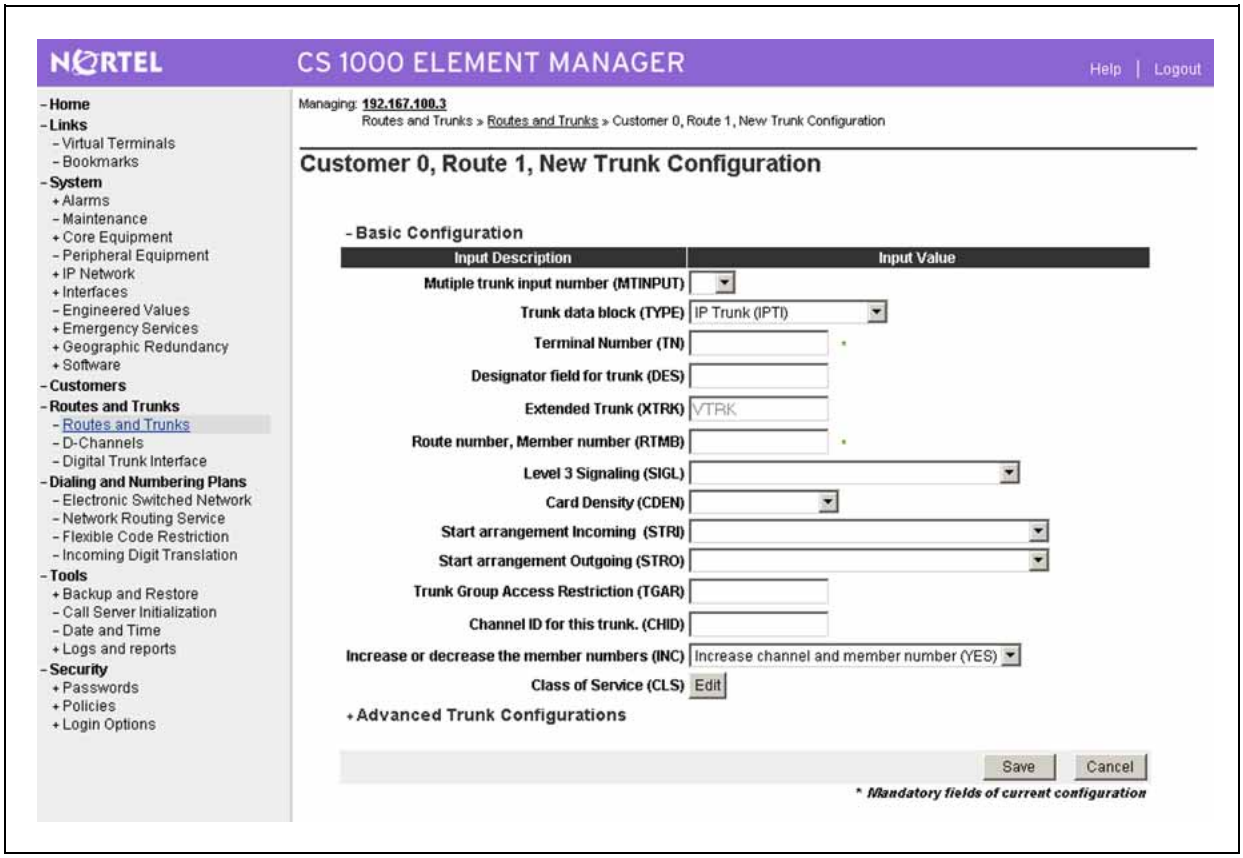
Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Routes and Trunks > Route and Trunks**, and select a customer record, as shown in Figure 4 "Routes and Trunks page" (page 55).

Figure 4
Routes and Trunks page



3 Click **Add Trunk** for the route to which you want to add a trunk. The New Trunk Configuration page appears, as shown in Figure 5 "New Trunk Configuration page" (page 56).

Figure 5
New Trunk Configuration page



4 From the **Trunk datablock type** menu, select **IP Trunk (IPT1)**.

5 In the **Extended Trunk (XTRK)** field, type **VTRK**.

6 Enter values in the **Terminal Number (TN)** and **Route number, Member number (RTMB)** fields.

7 Click **Edit** next to **Class of Service (CLS)**.

8 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.

Figure 6 "Media Security Class of Service menu" (page 57) shows the Media Security (CLS) menu and available Class of Service values.

Figure 6
Media Security Class of Service menu

9 Click **Return Class of Service**.

10 Click **Save**.

—End—

Media Security configuration information

Use the procedures in this section to access information about the configuration of the Media Security feature.

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.

Procedure 6
Viewing Media Security Settings using LD 117

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 15 "Job aid: commands to access information about Media Security configuration" (page 58).

—End—

Table 15
Job aid: commands to access information about Media Security configuration

Prompt	Response	Description
=>	PRT MSEC SYS	Prints the system-wide Media Security configuration. Prints if Media Security debug mode is enabled or disabled. Prints the remaining timeout value when the system automatically disables Media Security debug mode.
=>	PRT MSEC IP <ip_address>	Prints the Media Security Class of Service for a specified IP address. Prints if Media Security debug mode is enabled or disabled for the individual IP addresses and prints the remaining timeout values when Media Security debug mode for the IP addresses are automatically disabled. An IP address can be complete or partial. For example, PRT MSEC IP 47.11.0.0 prints the Media Security Class of Service for the IP Phones whose IP addresses are in the range from 47.11.0.0 to 47.11.255.255.
=>	PRT MSEC TN <tn>	Prints the Media Security Class of Service for a specified TN. Prints if Media Security debug mode is enabled or disabled for the individual terminals and prints the remaining timeout values when Media Security debug mode for the terminals are automatically disabled. A TN can be complete or partial. For example, PRT MSEC TN 61 prints the Media Security Class of Service for IP Phones whose TNs are in the range from (61, 0) to (61, maximum).
=>	PRT MSEC ALL	Prints the system-wide Media Security configuration, as well as the Media Security Class of Service for all TNs. Prints if Media Security debug mode is enabled or disabled. Prints the remaining timeout value when the system automatically disable Media Security debug mode. Prints if Media Security debug mode is enabled or disabled for the individual terminals and prints the remaining timeout values when Media Security debug mode for terminals are automatically disabled.

Use the following procedure to view information about system-wide Media Security settings using LD 22.

Procedure 7
Viewing system-wide Media Security settings using LD 22

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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.

Procedure 8
Viewing user level Class of Service settings using LD 11 or LD 20

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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	At the LD 20 or LD 11 `DATE` prompt, make no entry.
6	At the LD 20 or LD 11 `DES` prompt, make no entry.

—End—

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 9
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 49).
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.

Procedure 10
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—

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. SIP TLS provides protection of communication with IP Phones with SIP firmware, and IP Softphones. Use the procedures in this section to configure SIP TLS on your system. For more information about SIP TLS concepts and implementation in Communication Server 1000 (CS 1000) Release 5.0, see "TLS security for SIP trunks concepts" (page 34).

SIP TLS configuration overview

A typical configuration of a SIP-enabled CS 1000 Release 5.0 network consists of a SIP Proxy server or Linux-based NRS having one primary NRS and one alternate NRS, plus multiple SIP endpoints, and a primary and backup security server. To configure SIP TLS you must configure certificates for the SIP Proxy server and for the SIP endpoints before enabling SIP TLS.

In the following discussion, an element can be a SIP Proxy server or a SIP endpoint. To configure SIP TLS, carry out the following four steps:

- Deploy certificates for SIP Proxy server
  - In ECM, add a new element by using the steps in Procedure 15 "Adding an element" (page 75).
  - In ECM, add a certificate by using the steps in one of the following:

- "Create a certificate for SIP TLS signed by a local private CA " (page 100)
- "Create a certificate for SIP TLS signed by a trusted third-party CA " (page 105)
- "Create a self-signed certificate for SIP TLS " (page 113)

— If the system has an alternate NRS or SIP Proxy 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 122).
- In ECM, select the server to which you wish 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 125).
- 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 82).

• Enable TLS for SIP Proxy server

— If there is a firewall between the Security Server and the SIP Proxy Server, open the ports on the firewall to allow security certificate communication, as follows:

- TCP port 5061 for SIP TLS communication
- 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

— Complete the following steps only once for the system. You do not need to repeat them each time you configure an endpoint:

- In ECM, provision a security certificate for the primary SIP Proxy server
- In ECM, provision a security certificate for the alternate SIP Proxy server

- In NRSM, enable SIP Proxy to open TLS ports by using the information in *Network Routing Services Installation and Commissioning (NN43001-564)*.
- Restart the SIP Proxy service.

- Deploy certificates for SIP endpoints
  - In ECM, add a new element by using the steps in Procedure 15 "Adding an element" (page 75).
  - In ECM, add a certificate by using the steps in one of the following:
    - "Create a certificate for SIP TLS signed by a local private CA " (page 100)
    - "Create a certificate for SIP TLS signed by a trusted third-party CA " (page 105)
    - "Create a self-signed certificate for SIP TLS " (page 113)
  - 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 122).
    - In ECM, select the server to which you wish to add the certificate, and Import a certificate and it's key by using the steps in "Import a certificate and its private key from a file" (page 125).
    - 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 82).

- Enable TLS for SIP endpoints
  - If there is a firewall between the Security Server and the SIP endpoint, open the ports on the firewall to allow security certificate communication, as follows:
    - TCP port 5061 for SIP TLS communication
    - 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 gateway endpoints that use a static endpoint IP address:

- In NRSM, configure the gateway endpoints by using the information in *Network Routing Services Installation and Commissioning (NN43001-564)*.

— In Element Manager, provision a SIP gateway to use TLS as transport protocol, save and transfer the changes, and reboot the SIP Gateway by using the steps in "Configuring SIP TLS security policy" (page 67).

Use the CLI commands in "SIP TLS maintenance using CLI" (page 74) to check the configuration and status of the SIP/TLS connection.

Job aid: config.ini file

After you make changes using the procedures in this section, you can verify the changes by examining the config.ini file, which is stored on the SIP Gateway, in the following location: **`/u/config/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 16 "SIP TLS security parameters" (page 64).

Table 16
SIP TLS security parameters

Parameter	Possible values	Description
Security policy	0 = Security Disabled (Default) 1 = Best Effort	securityPolicy indicates the security policy SIP TLS uses:

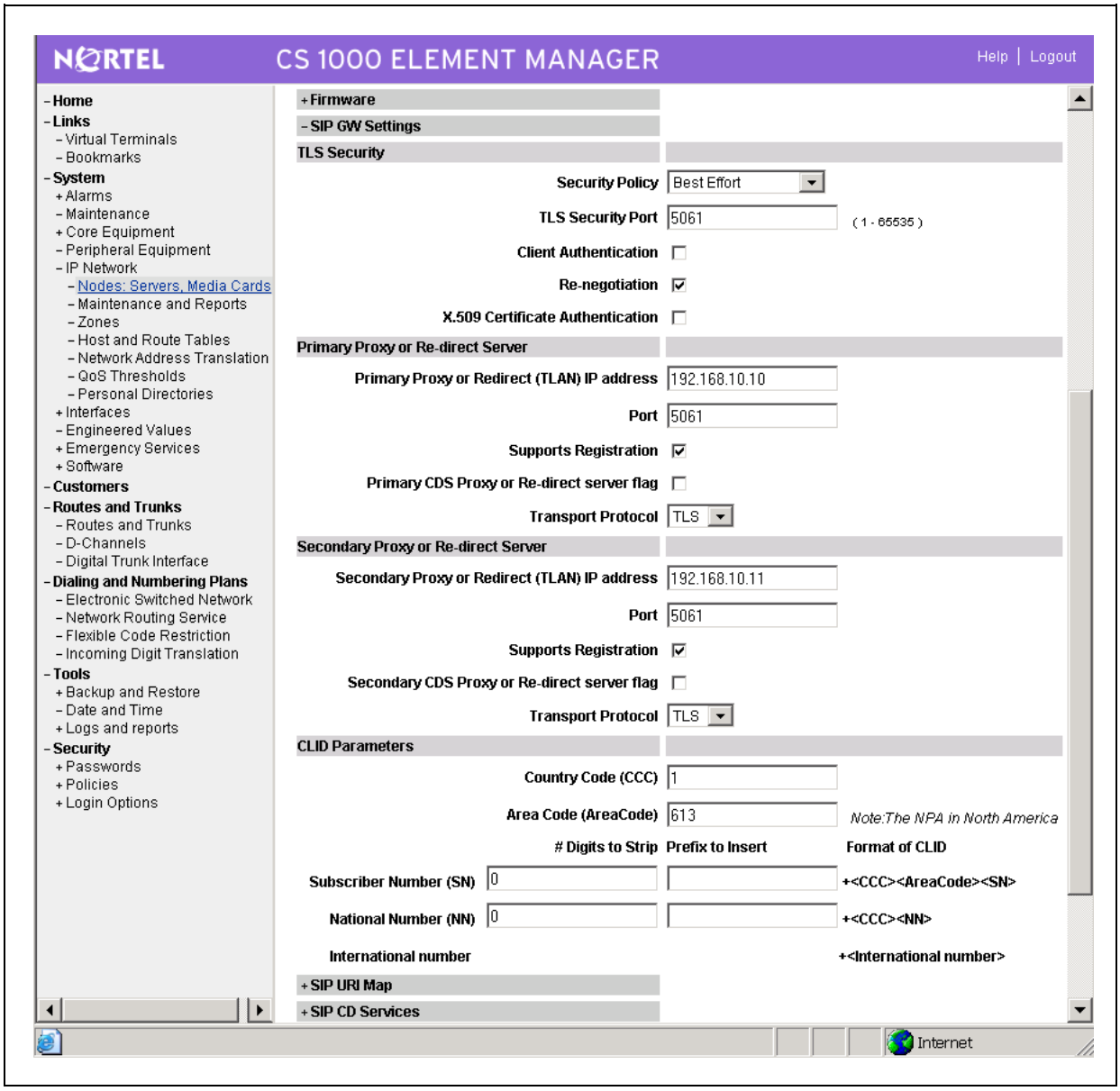
	2 = Secure Local 3 = Secure End to End	• Security Disabled turns SIP TLS off. The user can configure proxy transport to use TCP or UDP. • Best Effort turns SIP TLS on. The user can configure proxy transport to use TLS, TCP, or UDP. • Secure Local turns SIP TLS on. The user must configure proxy transport to use TLS. • Secure End to End turns SIP TLS on. Calls are only completed if you configure all nodes to use Secure End to End.
TLS Security Port	Default value is : 5061 Valid range is 1-65 535	tlsSecurityPort identifies the listening port that is used by TLS.
Client Authentication	0 = Disabled (Default) 1 = Enabled	clientAuthenticationEnabled indicates whether the system, when operating on the server side of the TLS connection, requires a certificate to be sent from the client side.
Renegotiation	0 = Disabled 20 000 000 = Enabled (Default)	numByteRenegotiation indicates whether the SIP TLS connection is renegotiated periodically to change the session key. The default is Enabled; renegotiation is triggered after 20 000 000 bytes have passed over the connection.
X.509 Certificate Authentication	0 = Disabled (Default) 1 = Enabled	x509CertAuthentication indicates whether the system, when operating on the client side of the SIP/TLS connection, accepts self-signed certificates from the server side. If you enable x509CertAuthentication, SIP TLS provides both encryption and identity verification. 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.

To access SIP Gateway (SIP GW) configuration options in Element Manager, go to **IP Networks > Nodes, Servers, Media Cards**. Click **Edit** next to the node you wish to edit, and then click **+ SIP GW Settings**. The SIP GW settings appear, as shown in Figure 7 "SIP GW settings in Element Manager" (page 66). Use the options on this screen to configure SIP TLS.

Figure 7
SIP GW settings in Element Manager



The security policy options for SIP TLS are described in Table 17 "Job aid: SIP TLS security policy descriptions" (page 67).

Table 17
Job aid: SIP TLS security policy descriptions

Security policy	Requirements
Secure End-to-End	To ensure call completion, this security policy works with CS 1000 networks only when all of the nodes are configured to use Secure End-to-End.
Secure Local (Guarantee local hop TLS)	You must configure Transport Protocol as TLS.
Best Effort (Best interoperability)	You can configure Transport Protocol as one of: TLS, TCP, or UDP.
Security Disabled (No SIP TLS security)	You can configure Transport Protocol as TCP or UDP.
Note: If you use Secure End-to-End policy or Secure Local policy, Failsafe Redirect Server is not supported.	

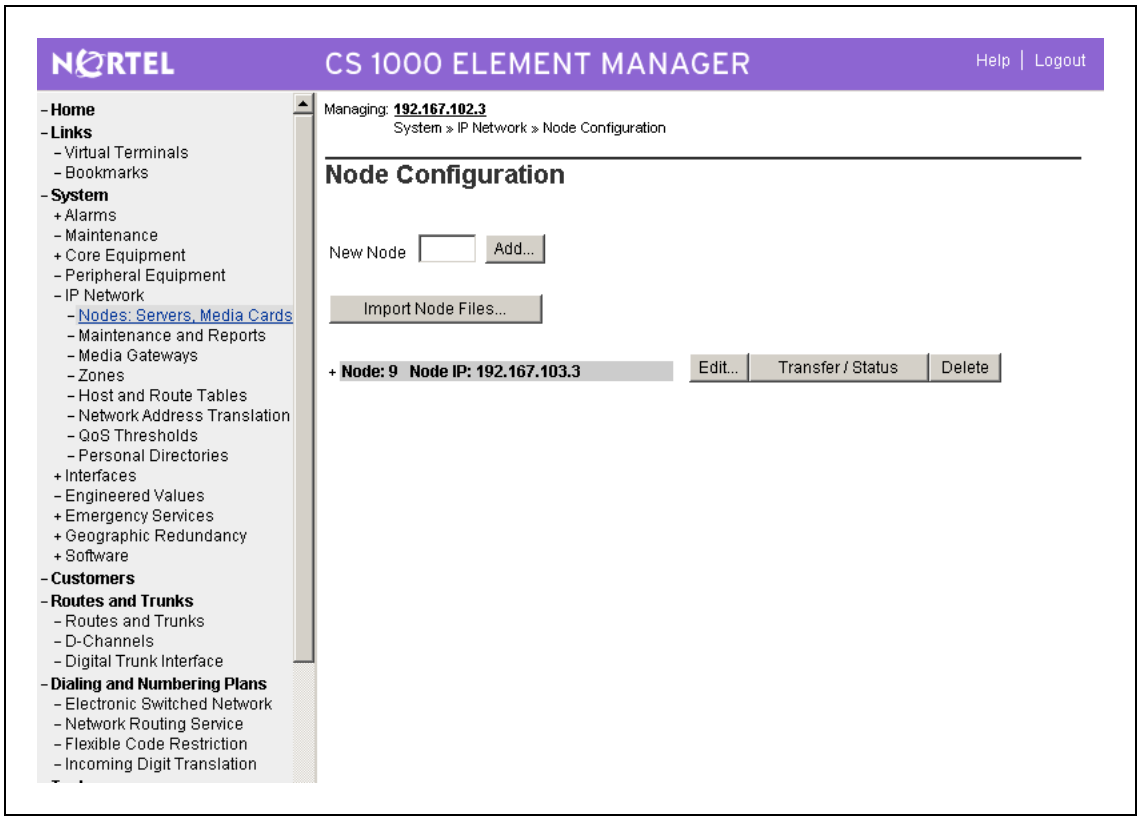
Configuring SIP TLS security policy

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

Procedure 11
Configuring TLS to Security disabled by using Element Manager

Step	Action
1	Log on to Element Manager.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears, as shown in Figure 8 "Node Configuration " (page 68).

Figure 8
Node Configuration

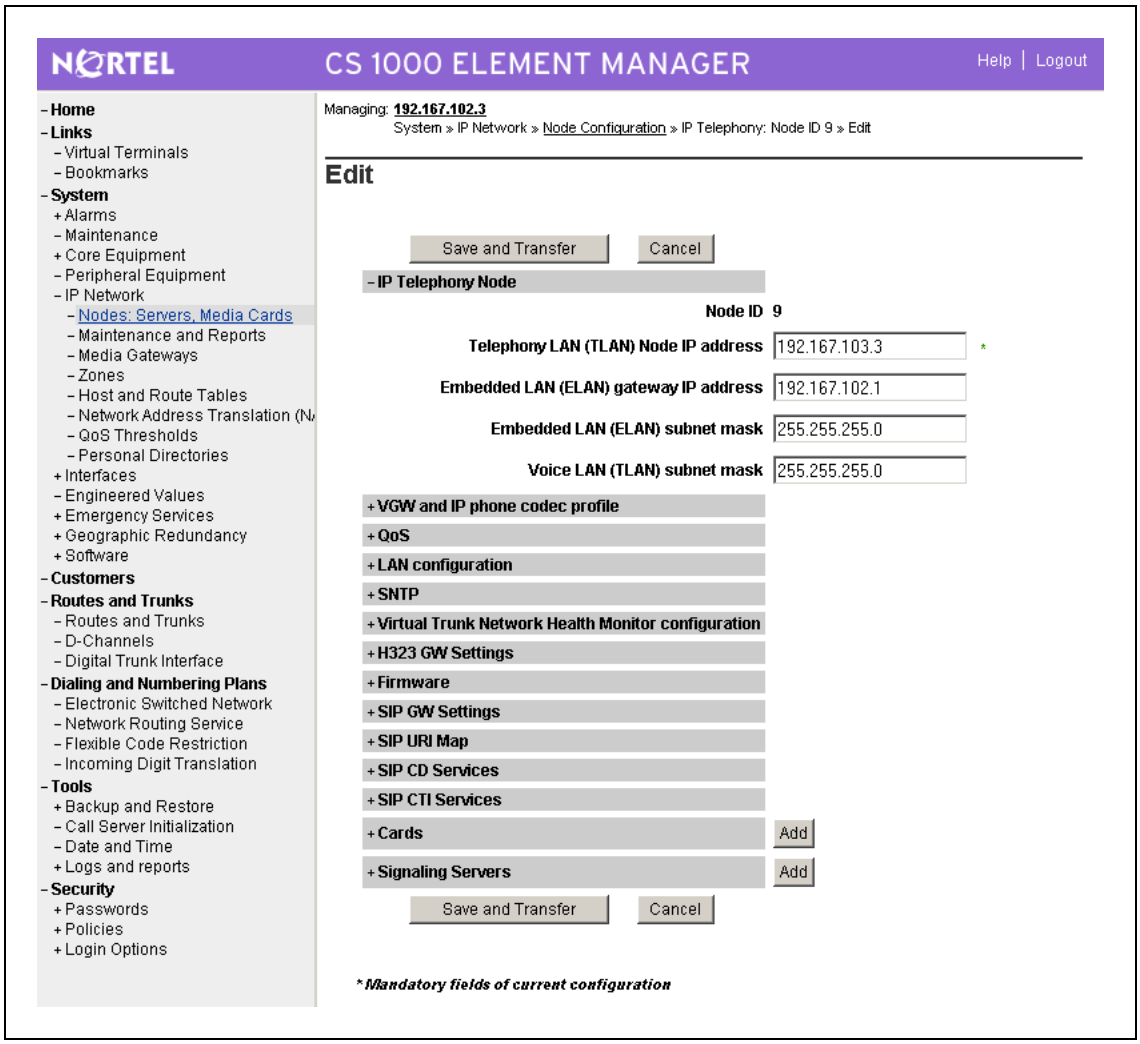


3 Enter a node number.

4 Click **Edit**.

The **Edit Node** page appears as shown in Figure 9 "Edit Node" (page 69).

Figure 9
Edit Node



5 Expand the **SIP GW Settings** option as shown in Figure 7 "SIP GW settings in Element Manager" (page 66).

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

For more information about available security policies, see Table 17 "Job aid: SIP TLS security policy descriptions" (page 67).

7 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 16 "SIP TLS security parameters" (page 64).

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

9 Type appropriate values in the remaining fields on the page.

10 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>.
```

11 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 "Job aid: config.ini file" (page 64).

Procedure 12

Configuring TLS to Best effort by using Element Manager

Step	Action
1	Log on to Element Manager.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears, as shown in Figure 8 "Node Configuration " (page 68).
3	Enter a node number.
4	Click **Edit**. The **Edit Node** page appears as shown in Figure 9 "Edit Node" (page 69).
5	Expand the **SIP GW Settings** option as shown in Figure 7 "SIP GW settings in Element Manager" (page 66).
6	In the **TLS Security** section, use the **Security Policy** menu to choose **Best effort**. For more information about available security policies, see Table 17 "Job aid: SIP TLS security policy descriptions" (page 67).
7	In the **TLS Security Port** field, type `5061`.

For more information about TLS parameters, see Table 16 "SIP TLS security parameters" (page 64).

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

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

10 Optionally, select the **X509 Certificate Authentication** button to enable it.

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

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

13 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>.
```

14 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 "Job aid: config.ini file" (page 64).

Procedure 13
Configuring TLS to Secure Local by using Element Manager

Step	Action
1	Log on to Element Manager.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears, as shown in Figure 8 "Node Configuration " (page 68).
3	Enter a node number.
4	Click **Edit**. The **Edit Node** page appears as shown in Figure 9 "Edit Node" (page 69).

5 Expand the **SIP GW Settings** option as shown in Figure 7 "SIP GW settings in Element Manager" (page 66).

6 In the **TLS Security** section, use the **Security Policy** menu to choose **Secure Local**.

For more information about available security policies, see Table 17 "Job aid: SIP TLS security policy descriptions" (page 67).

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

For more information about TLS parameters, see Table 16 "SIP TLS security parameters" (page 64).

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

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

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

ATTENTION

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

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

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

13 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>.
```

14 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 "Job aid: config.ini file" (page 64).

Procedure 14
Configuring TLS to Secure End to End by using Element Manager

Step	Action
1	Log on to Element Manager.
2	Click **System > IP Network > Nodes: Servers, Media Cards**. The **Node Configuration** page appears, as shown in Figure 8 "Node Configuration " (page 68).
3	Enter a node number.
4	Click **Edit**. The **Edit Node** page appears as shown in Figure 9 "Edit Node" (page 69).
5	Expand the **SIP GW Settings** option as shown in Figure 7 "SIP GW settings in Element Manager" (page 66).
6	In the **TLS Security** section, use the **Security Policy** menu to choose **Secure End to End**. For more information about available security policies, see Table 17 "Job aid: SIP TLS security policy descriptions" (page 67).
7	In the **TLS Security Port** field, type `5061`. For more information about TLS parameters, see Table 16 "SIP TLS security parameters" (page 64).
8	Verify that the **Re-negotiation** option button is selected.
9	Optionally, select the **Client Authentication** option button to enable it.
10	Optionally, select the **X509 Certificate Authentication** option button to enable it.
11	In the **Primary Proxy** section, type `5061` in the **Port** field, and configure **Transport Protocol** to **TLS**.
12	In the **Secondary Proxy** section, type `5061` in the **Port** field, and configure **Transport Protocol** to **TLS**.
13	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>.`

14 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 "Job aid: config.ini file" (page 64).

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 "Security certificates" (page 75).

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.

Security certificates

This chapter contains procedures to help you manage certificate authorities (CA) and security 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 security certificate concepts, Web SSL, and SIP TLS in Communication Server 1000 (CS 1000) Release 5.0, see "Security certificate concepts" (page 37).

Add an element

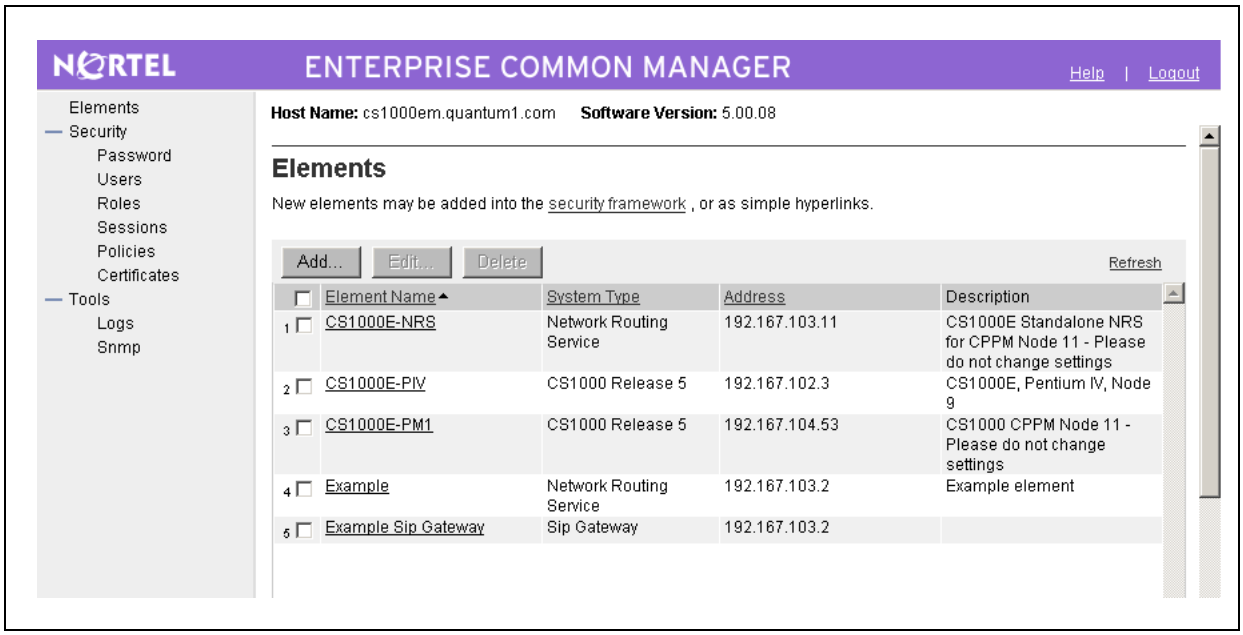
The procedures in this chapter are performed on elements. If you wish to manage certificates or certificate authorities (CA) for elements that do not already exist, use Procedure 15 "Adding an element" (page 75) to add an element. For more information about managing elements, see *Enterprise Common Manager Fundamentals (NN43001-116)*.

Procedure 15
Adding an element

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, as shown in Figure 10 "Elements" (page 76).

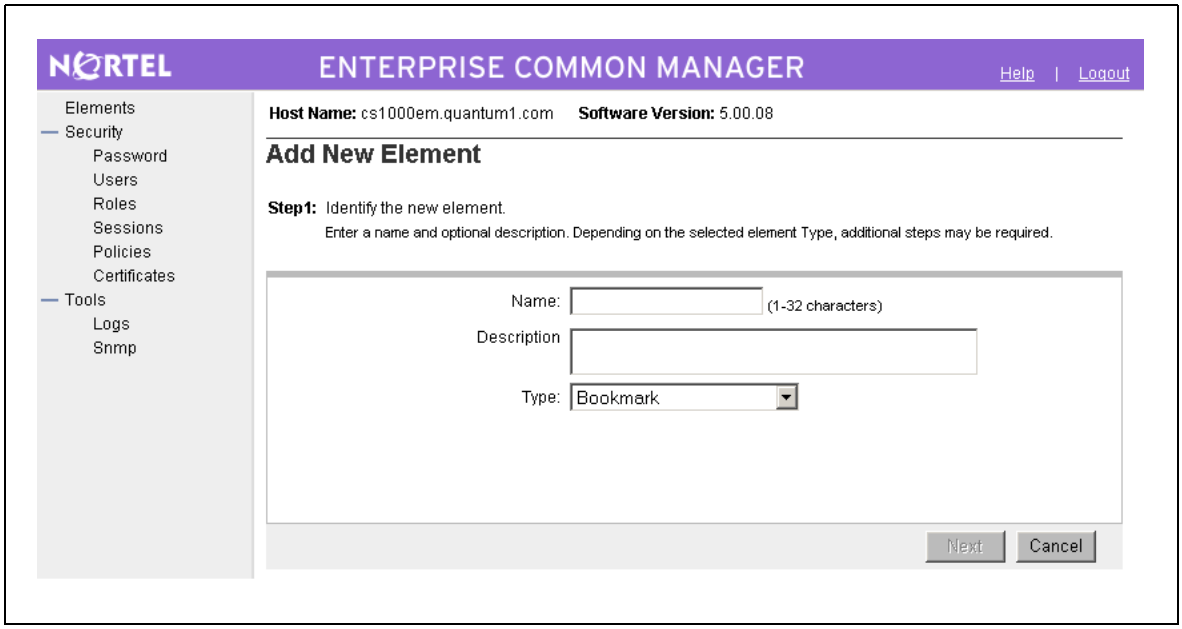
Figure 10
Elements



3 Click the **Add** button.

The **Add New Element step 1** page appears, as shown in Figure 11 "Add New Element step 1" (page 76).

Figure 11
Add New Element step 1

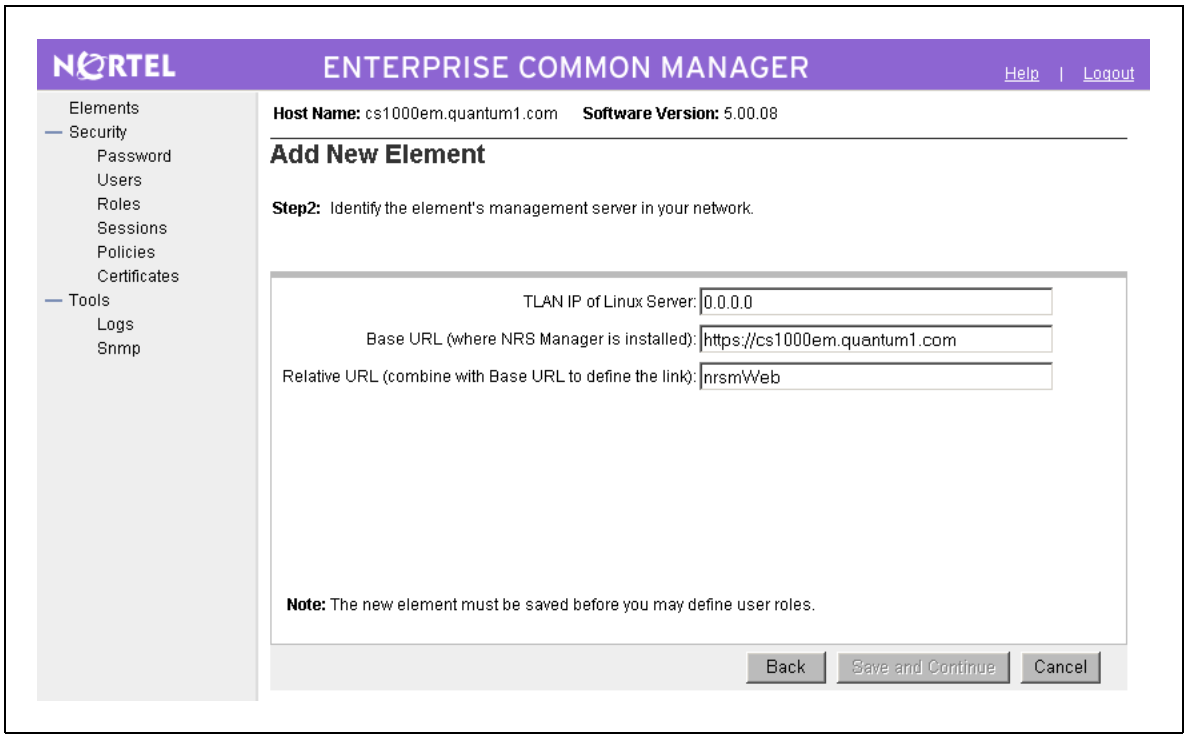


4 Perform the following actions:

- In the **Name** field, type an element name.
- In the **Description** field, type a description.
- From the **Type**: list, choose one of **Network Routing Service** (for SIP Proxy) or **SIP Gateway.**

5 Click **Next**. The **Add New Element step 2** page appears, as shown in Figure 12 "Add New Element step 2" (page 77).

Figure 12
Add New Element step 2

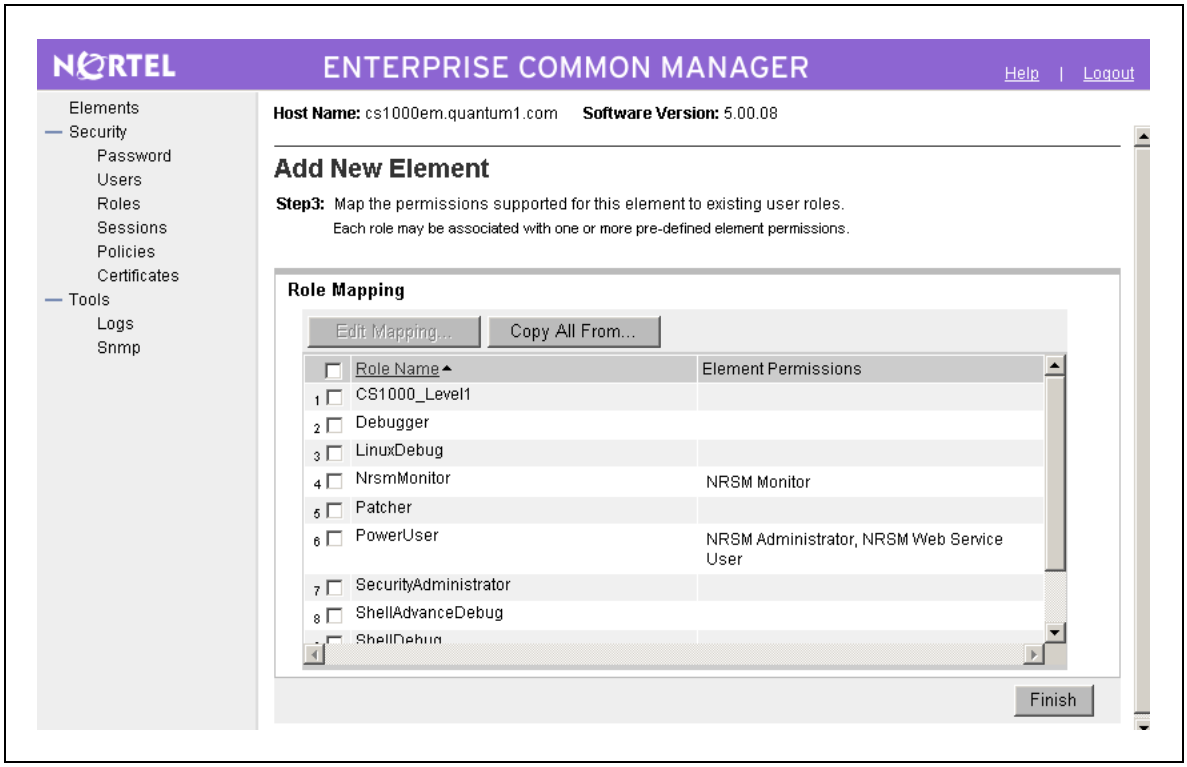


6 Perform the following actions:

- In the **TLAN IP of the Linux server** field, type the TLAN IP.
- In the **Base URL (where NRS Manager is installed)** field, type the NRS Manager URL.
- In the **Relative URL (combine with Base URL to define the link)** field, type the relative URL.

7 Click **Save and Continue**. The **Add New Element step 3** page appears, as shown in Figure 13 "Add New Element step 3" (page 78).

Figure 13
Add New Element step 3



8 Assign permissions for the new element by selecting from the roles listed in the **Role Mapping** pane.

9 Click **Finish**.

—End—

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)*.

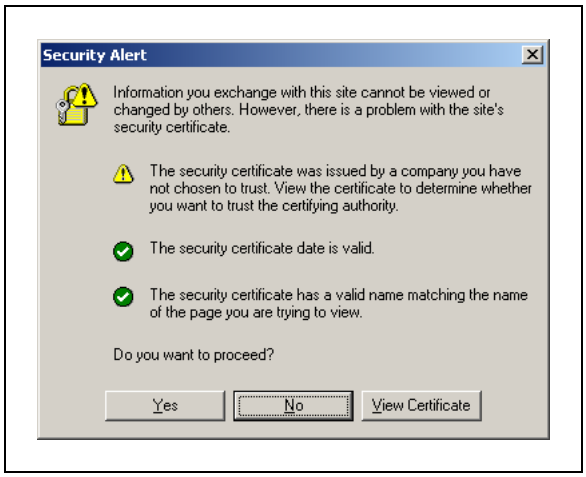
During the primary security service installation, a Web SSL certificate is issued from the private CA that is installed as part of the primary security service. Use that certificate for the ECM Web server, the Sun Access Manager Web server, and the LDAP server.

Use the following procedure to access the primary security server.

Procedure 16
Accessing the Web server 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, as shown in Figure 14 "CA is not in the trusted list" (page 79), stating that the private CA installed on the primary security server is not in the trusted CA list in the Web browser.

Figure 14
CA is not in the trusted list



2	If the Figure 14 "CA is not in the trusted list" (page 79) Security Alert window appears, add the private CA to the trusted CA list in the Web browser using Procedure 18 "Install a certificate into the trusted CA list in the Web browser" (page 81).
3	Click **Yes** to proceed.

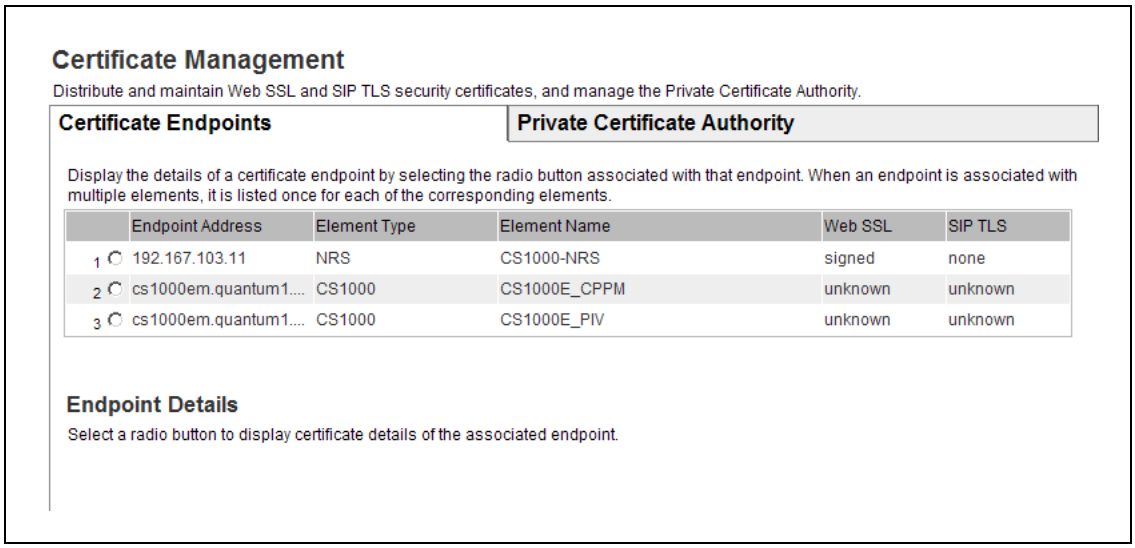
—End—

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

Procedure 17
Viewing private CA details

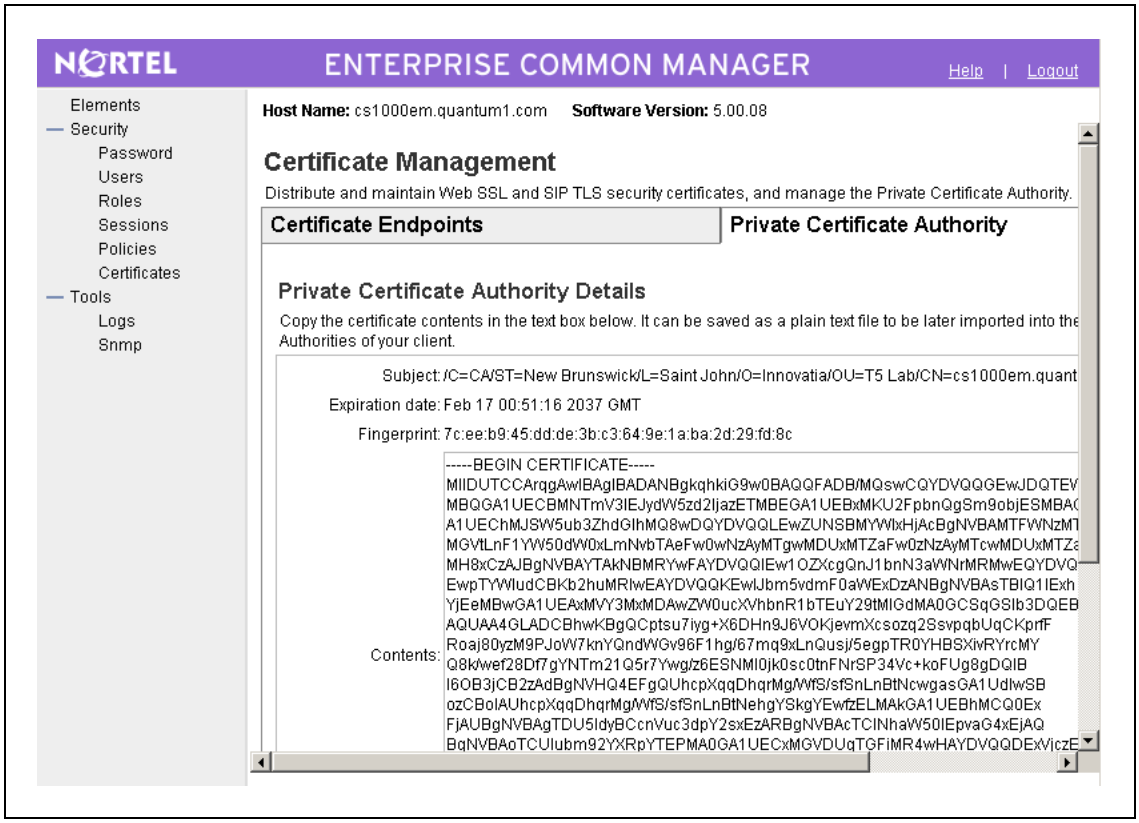
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears, as shown in Figure 15 "Certificate Management " (page 80).

Figure 15
Certificate Management



3	Click the **Private Certificate Authority** tab. The **Private Certificate Authority Details** page appears, as shown in Figure 16 "Private Certificate Authority Details " (page 81).

Figure 16
Private Certificate Authority Details



—End—

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

Procedure 18
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, as shown in Figure 15 "Certificate Management " (page 80).
3	Click the **Private Certificate Authority** tab.

The **Private Certificate Authority Details** page appears, as shown in Figure 16 "Private Certificate Authority Details " (page 81).

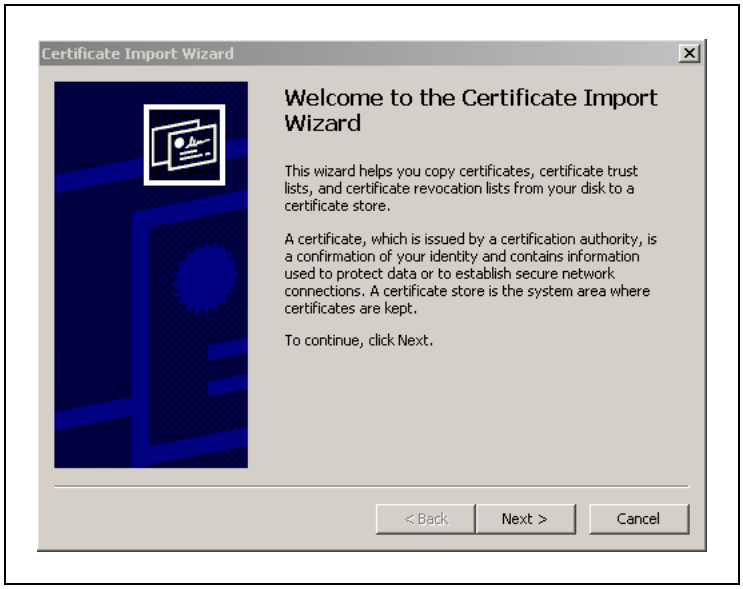
To copy the certificate information, click in the details window, press **Ctrl+a** to select all of the text, and then press **Ctrl+c** to copy the text.

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 as shown in Figure 17 "Certificate Import Wizard" (page 82).

Figure 17
Certificate Import Wizard



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

—End—

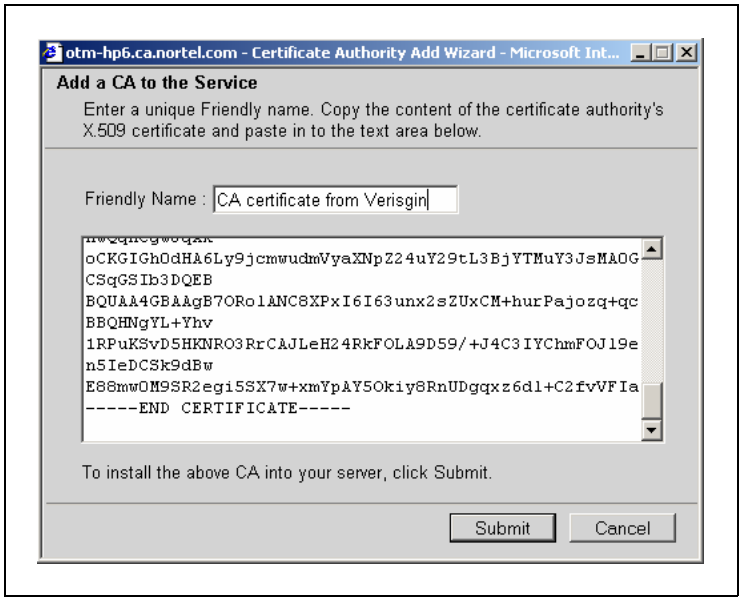
Add a CA to an endpoint

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

Procedure 19
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, as shown in Figure 15 "Certificate Management " (page 80).
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, as shown in Figure 18 "Add a CA to the Service" (page 83).

Figure 18
Add a CA to the Service



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 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—End—

Change the trust status of an endpoint

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

Procedure 20
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, as shown in Figure 15 "Certificate Management " (page 80).
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	Reboot the server that you changed in this procedure. The changes take effect only after the server reboots.

—End—

Delete a CA

Use the following procedure to delete a CA.

Procedure 21
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, as shown in Figure 15 "Certificate Management " (page 80).
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 one of: **OK** to proceed with the deletion **OR** **Cancel** to cancel the deletion.
7	Reboot the server that you changed in this procedure. The changes take effect only after the server reboots.

—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 18 "Certificate Management Wizard configuration options" (page 85).

Table 18
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 19 "Status types for certificate endpoints" (page 86).

Table 19
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.
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

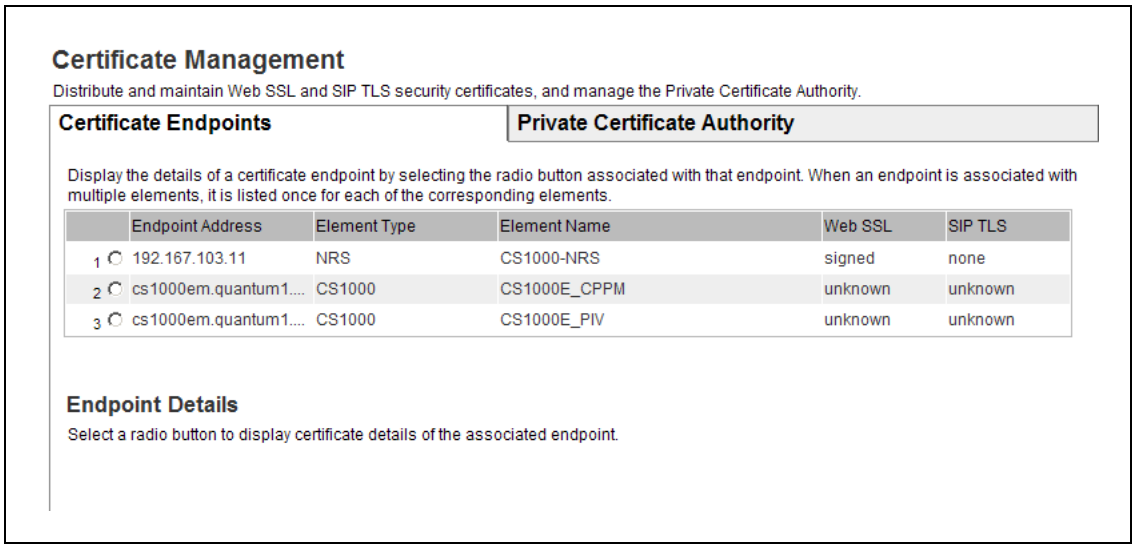
Use the following procedure to view the details about certificate endpoints and CAs.

Procedure 22

Viewing certificate details for an endpoint by using ECM

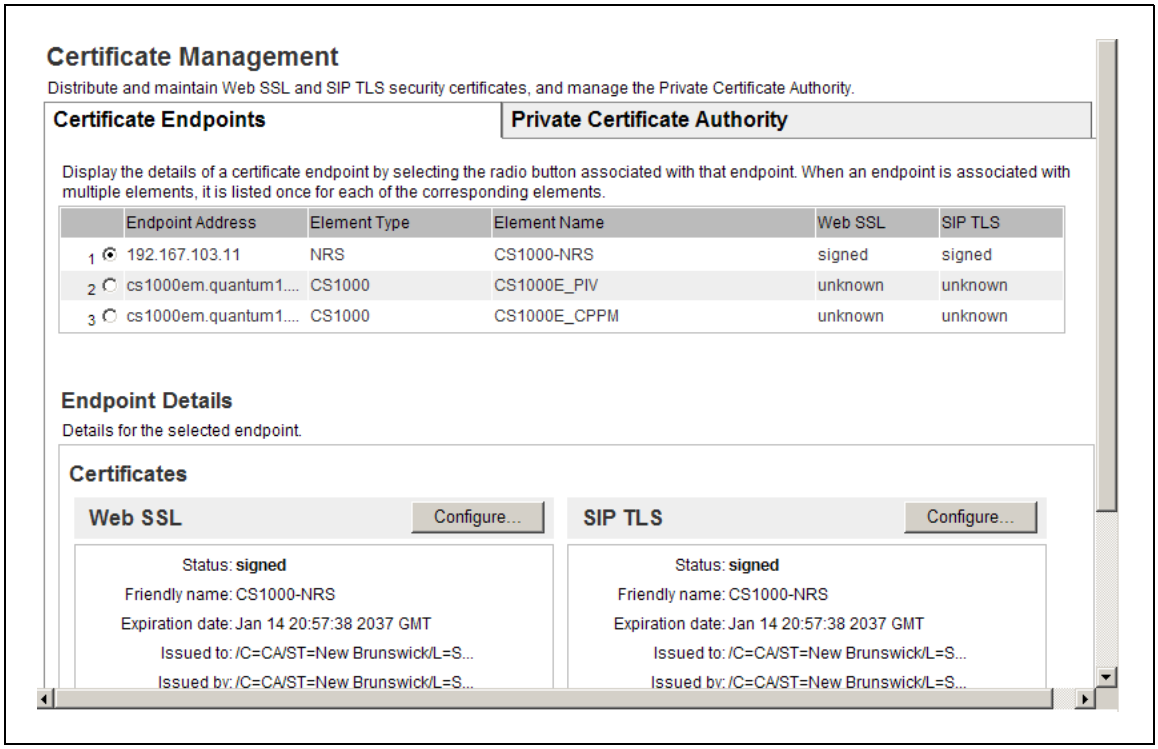
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears, as shown in Figure 19 "Certificate Management " (page 87).

Figure 19
Certificate Management



3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).

Figure 20
Endpoint Details



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 19 "Status types for certificate endpoints" (page 86).

—End—

Create a certificate for Web SSL signed by a local private CA

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

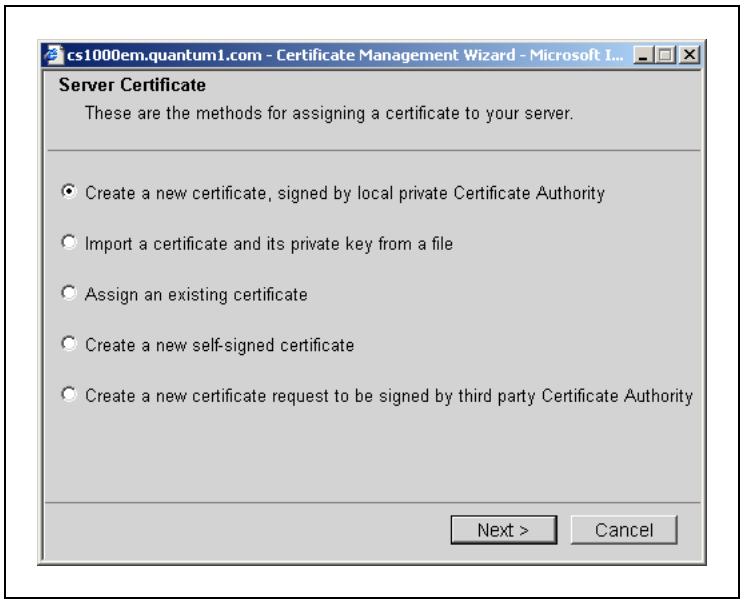
Prerequisites

- Certificates are added to elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).
- 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 19 "Status types for certificate endpoints" (page 86).

Procedure 23
Creating a certificate for Web SSL signed by a local 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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Certificates** pane, click the **Configure** button to the right of **Web SSL**. The **Server Certificate** window appears, as shown in Figure 21 "Server Certificate window when no certificate is installed" (page 89).

Figure 21
Server Certificate window when no certificate is installed



5	Select **Create a new certificate, signed by local private Certificate Authority** and click **Next**. The **Name and Security Settings** window appears, as shown in Figure 22 "Name and Security Settings" (page 90).

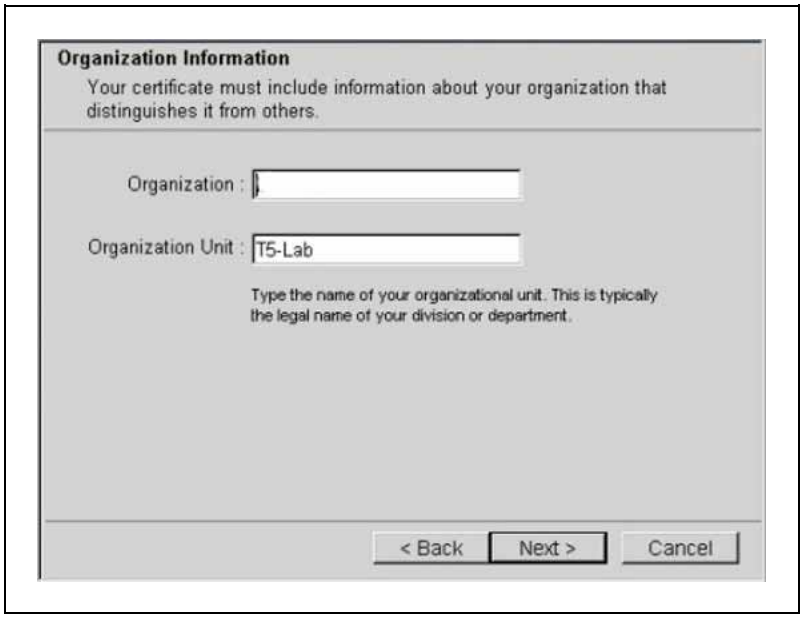
Figure 22
Name and Security Settings

6 In the **Name and Security Settings** window, perform the following tasks:

- In the **Friendly Name** field, enter a name.
- In the **Bit Length** list, choose a bit length. The default value is 1024.
- Click **Next**.

The **Organization Information** window appears, as shown in Figure 23 "Organization Information" (page 91).

Figure 23
Organization Information

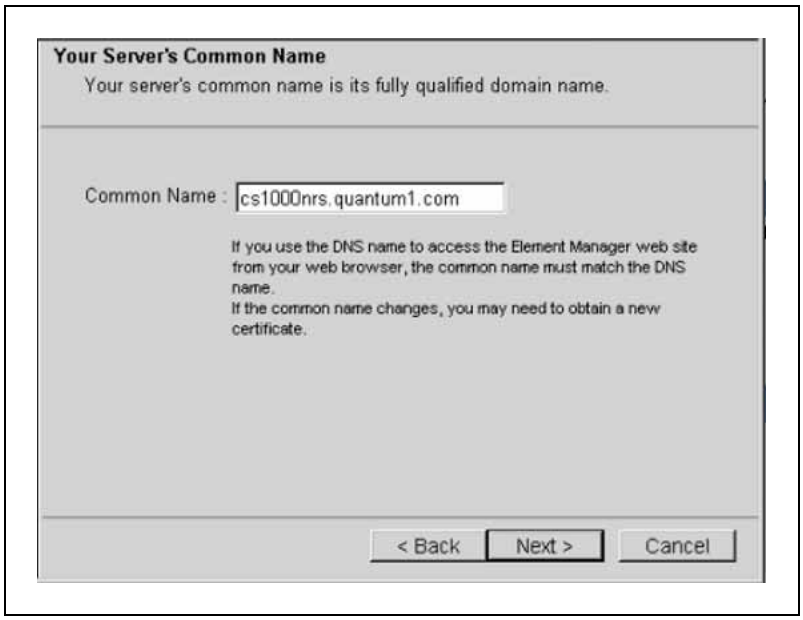


7 In the **Organization Information** window, perform the following tasks:

- 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, as shown in Figure 24 "Your Servers Common Name" (page 92).

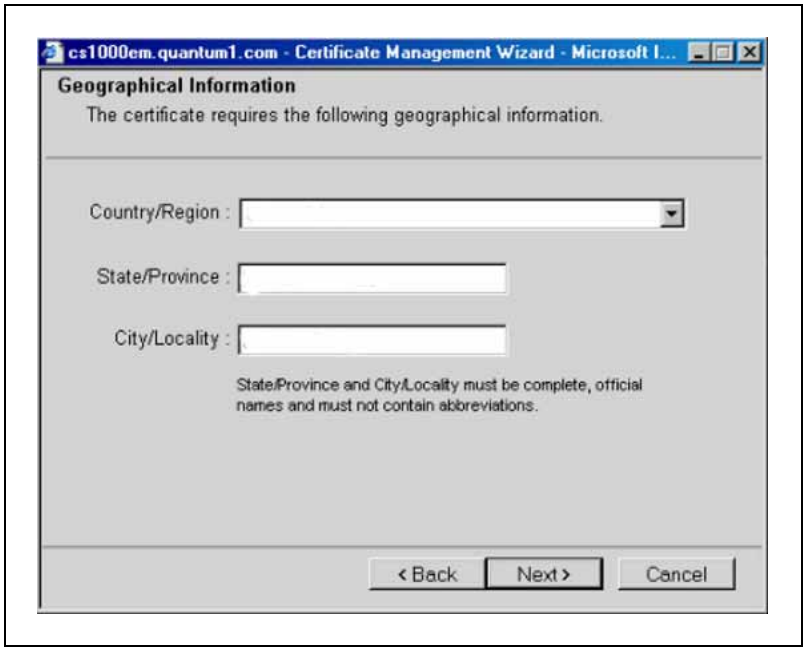
Figure 24
Your Servers Common Name



8 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, as shown in Figure 25 "Geographical Information" (page 92).

Figure 25
Geographical Information

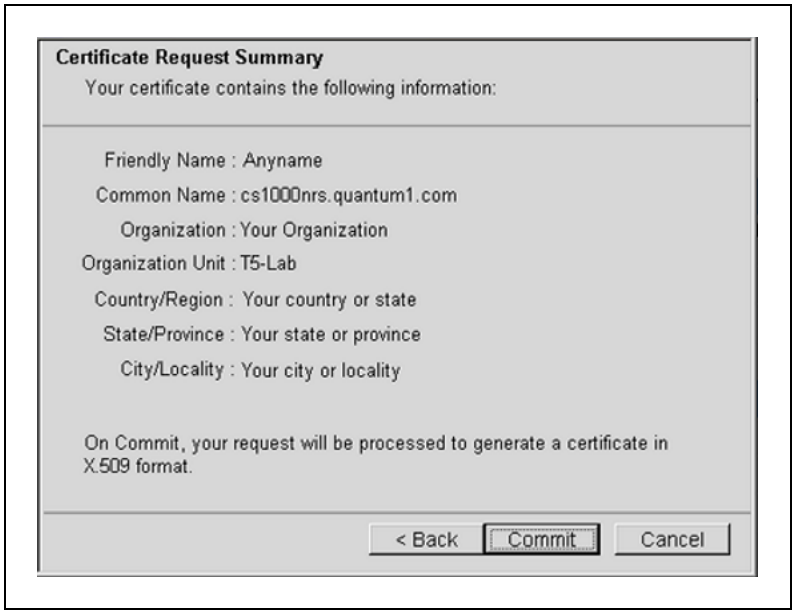


9 In the **Geographical Information** window, perform the following tasks:

- 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, as shown in Figure 26 "Certificate Request Summary" (page 93).

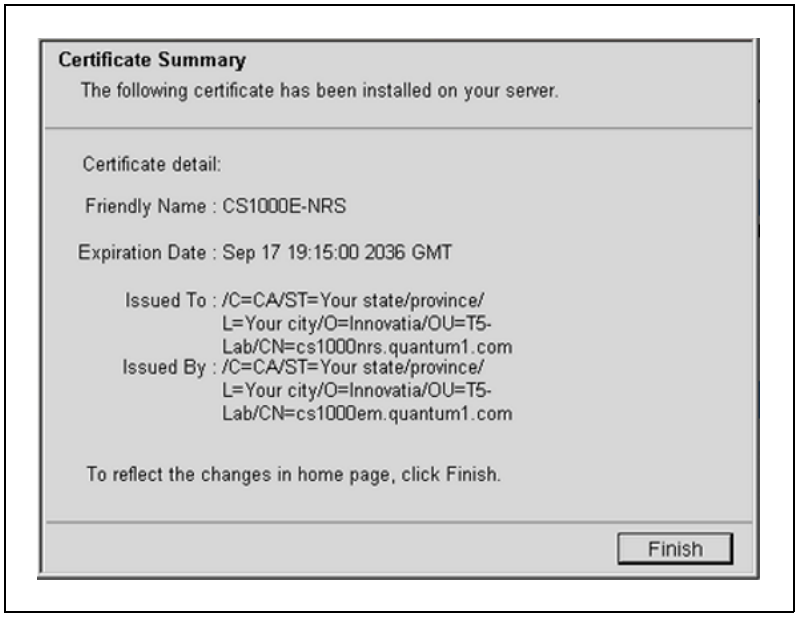
Figure 26
Certificate Request Summary



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

The **Certificate Summary** window appears with the certificate information, as shown in Figure 27 "Certificate Summary" (page 94).

Figure 27
Certificate Summary



11 Click **Finish**.

The status changes to signed.

12 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—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 elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).
- 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 19 "Status types for certificate endpoints" (page 86).

Procedure 24

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** section of the **Certificates** pane, click **Configure**. The **Server Certificate** window appears, as shown in Figure 21 "Server Certificate window when no certificate is installed" (page 89).
5	Select **Create a new certificate request to be signed by third party** and click **Next**. The **Name and Security Settings** window appears as shown in Figure 22 "Name and Security Settings" (page 90).
6	In the **Name and Security Settings** window, perform the following tasks: • In the **Friendly Name** field, enter a name. • In the **Bit Length** list, choose a bit length. The default value is 1024. • Click **Next**. The **Organization Information** window appears, as shown in Figure 23 "Organization Information" (page 91).
7	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, as shown in Figure 24 "Your Servers Common Name" (page 92).

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

The **Geographical Information** window appears.

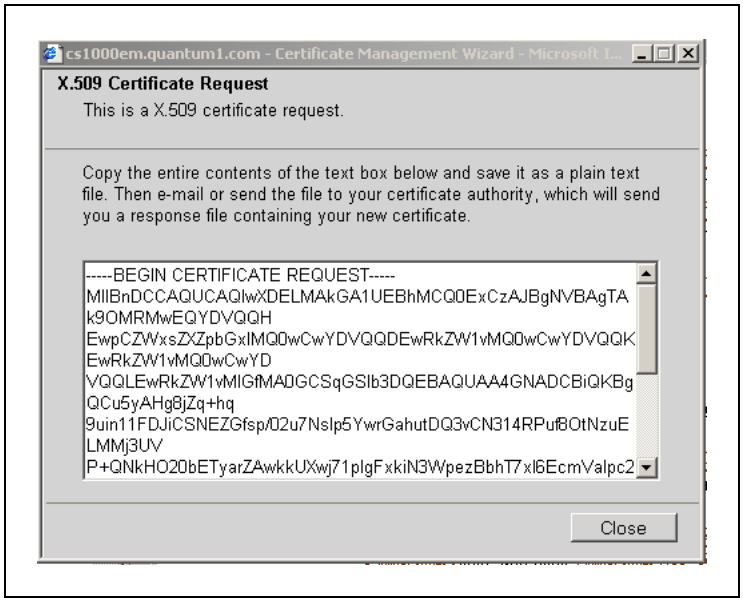
9 In the **Geographical Information** , perform the following tasks:

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

The **Certificate Request Summary** window appears, as shown in Figure 26 "Certificate Request Summary" (page 93).

10 Click **Commit**. The **X.509 Certificate Request** window appears, as shown in Figure 28 "X.509 Certificate Request" (page 96)

Figure 28
X.509 Certificate Request



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

11 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.

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

13 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.

14 To process the pending request and install the certificate, follow the steps in Procedure 31 "Processing a pending certificate request by using ECM" (page 116).

The status changes to signed.

15 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—End—

After you reboot the system, a Security Alert appears, as shown in Figure 14 "CA is not in the trusted list" (page 79). Carry out the following two actions:

- Follow the instructions from the third-party vendor to download the intermediate CA.
- Follow the steps in Procedure 19 "Adding a CA to an endpoint" (page 83) 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 elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).
- 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 19 "Status types for certificate endpoints" (page 86).

Procedure 25

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, as shown in Figure 19 "Certificate Management " (page 87).

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

The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).

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

The **Server Certificate** window appears, as shown in Figure 21 "Server Certificate window when no certificate is installed" (page 89).

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

The **New Self-Signed Certificate** window appears as shown in Figure 29 " New Self Signed Certificate" (page 98).

Figure 29
New Self Signed Certificate

6 Click **Next**.

The **Name and Security Settings** window appears, as shown in Figure 22 "Name and Security Settings" (page 90).

7 Enter a **Friendly Name** for the certificate.

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

9 Click **Next**.

The **Organization Information** window appears as shown in Figure 23 "Organization Information" (page 91).

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 as shown in Figure 24 "Your Servers Common Name" (page 92).

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

The **Geographical Information** window appears as shown in Figure 25 "Geographical Information" (page 92).

12 Enter a **Country/Region**.

13 Enter a **State/Province**.

14 Enter a **City/Locality**.

15 Click **Next**.

The **Certificate Request Summary** window appears as shown in Figure 26 "Certificate Request Summary" (page 93).

16 Click **Commit**.

The **Certificate Summary** window appears as shown in Figure 27 "Certificate Summary" (page 94).

17 Click **Finish**.

The status changes to self-signed.

18 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—End—

After you reboot the system, a Security Alert appears, as shown in Figure 14 "CA is not in the trusted list" (page 79). Carry out the following two actions:

- Follow the steps in Procedure 34 "Exporting the current self-signed certificate by using ECM" (page 121) to export the self-signed certificate.

- Follow the steps in Procedure 19 "Adding a CA to an endpoint" (page 83) to add the self-signed certificate into the trusted CA list for the web browser.

Create a certificate for SIP TLS signed by a local private CA

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

Prerequisites

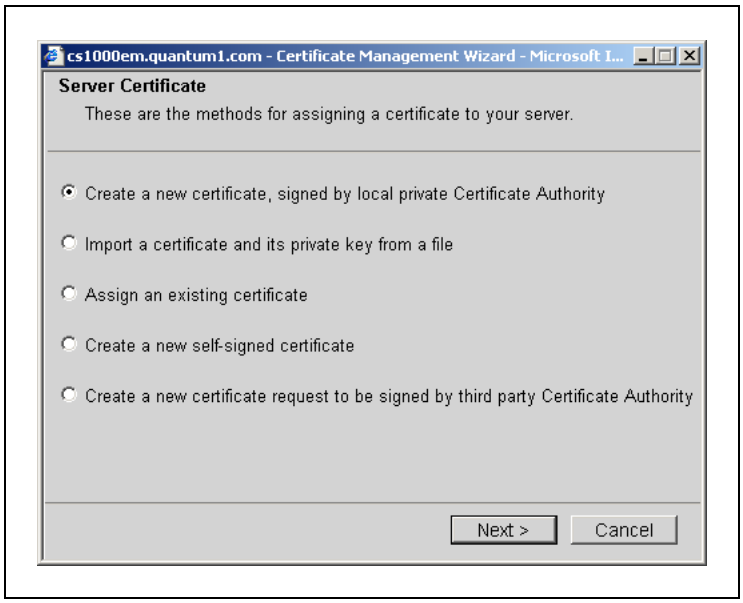
- Certificates are added to elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).
- Before you create a request for a new certificate signed by a local CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 19 "Status types for certificate endpoints" (page 86).

Procedure 26

Creating a certificate for SIP TLS signed by a local private CA

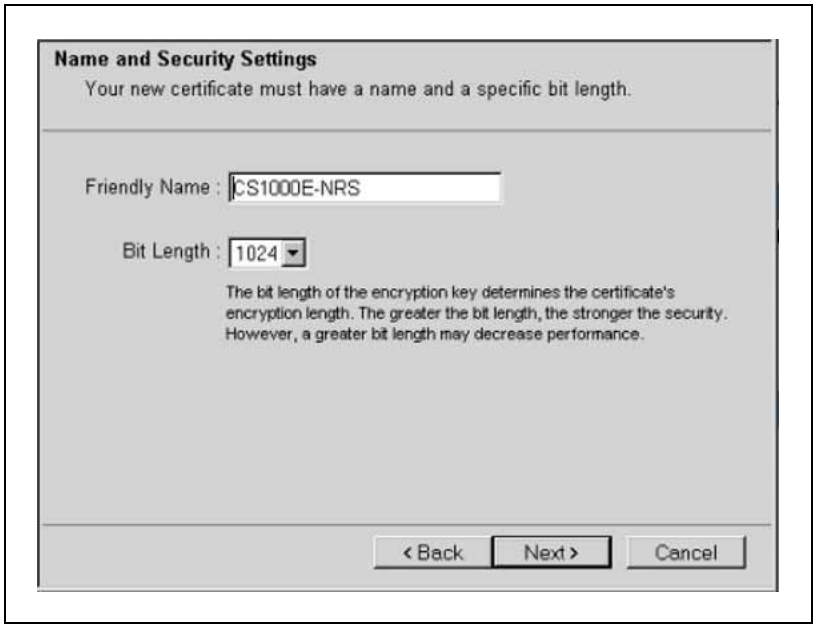
Step	Action
1	Click **Security** > **Certificates**. The **Certificate Management** page appears, as shown in Figure 19 "Certificate Management " (page 87).
2	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
3	In the **Certificates** pane, click the **Configure** button to the right of **SIP TLS**. The **Server Certificate** window appears, as shown in Figure 21 "Server Certificate window when no certificate is installed" (page 89).
4	Select **Create a new certificate, signed by local private Certificate Authority** and click **Next**, as shown in Figure 30 "Server Certificate window when no certificate is installed " (page 101).

Figure 30
Server Certificate window when no certificate is installed



The **Name and Security Settings** window appears, as shown in Figure 31 "Name and Security Settings" (page 101).

Figure 31
Name and Security Settings



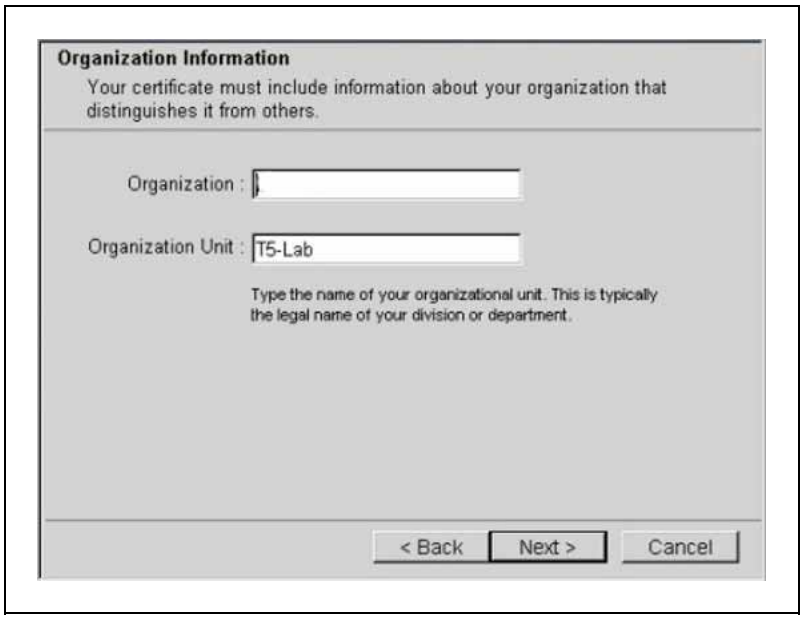
5 In the **Name and Security Settings** window, perform the following tasks:

- In the **Friendly Name** field, enter a name.

- From the **Bit Length** list, choose a bit length. The default value is 1024.
- Click **Next**.

The **Organization Information** window appears, as shown in Figure 32 "Organization Information" (page 102).

Figure 32
Organization Information

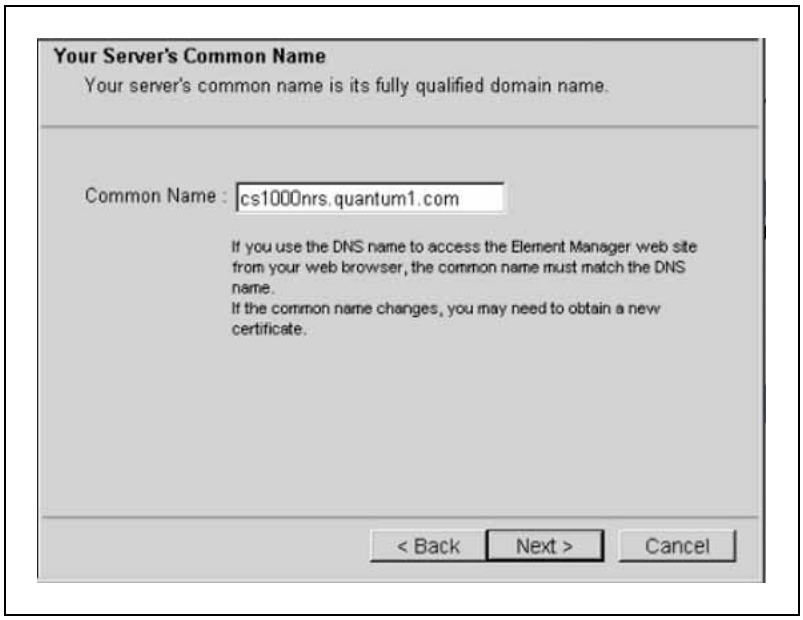


6 In the **Organization Information** window, perform the following tasks:

- 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, as shown in Figure 33 "Your Servers Common Name" (page 103).

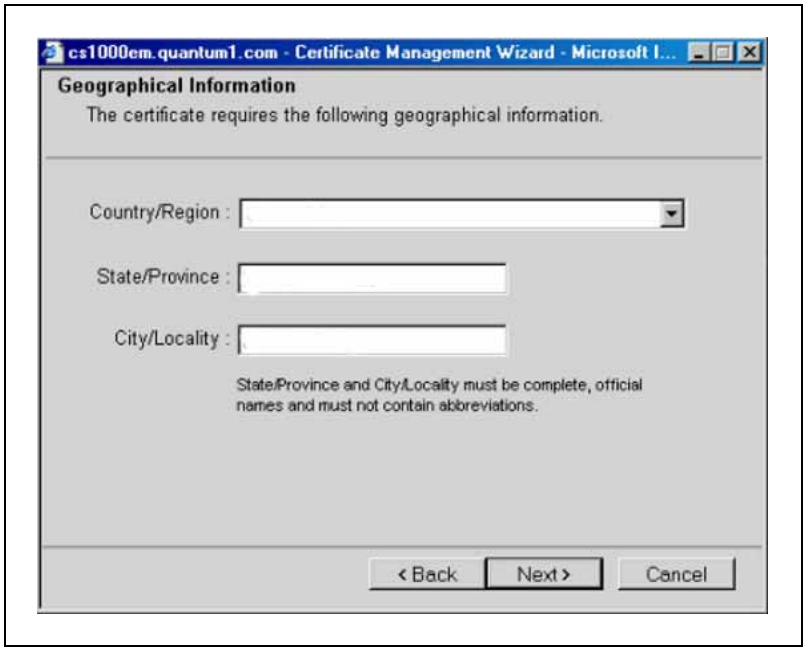
Figure 33
Your Servers Common Name



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

The **Geographical Information** window appears, as shown in Figure 34 "Geographical Information" (page 103).

Figure 34
Geographical Information

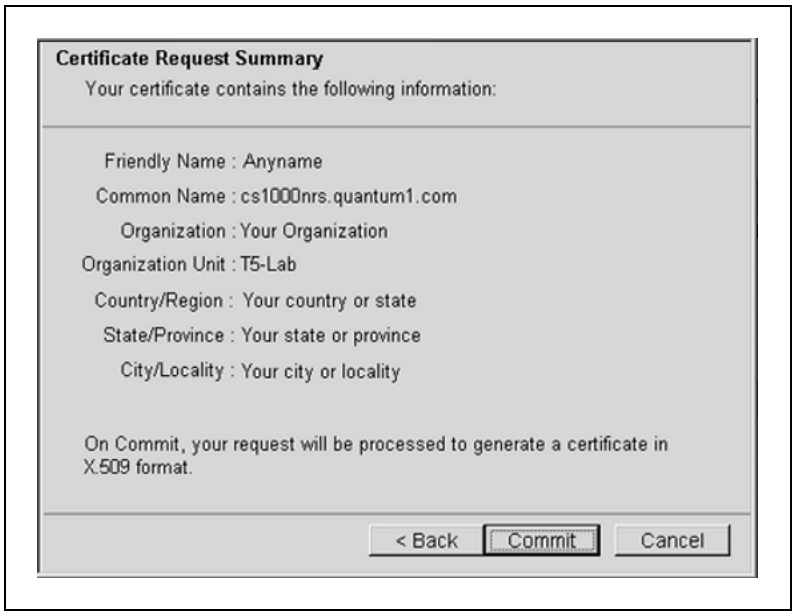


8 In the **Geographical Information** window, perform the following tasks:

- 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, as shown in Figure 35 "Certificate Request Summary" (page 104).

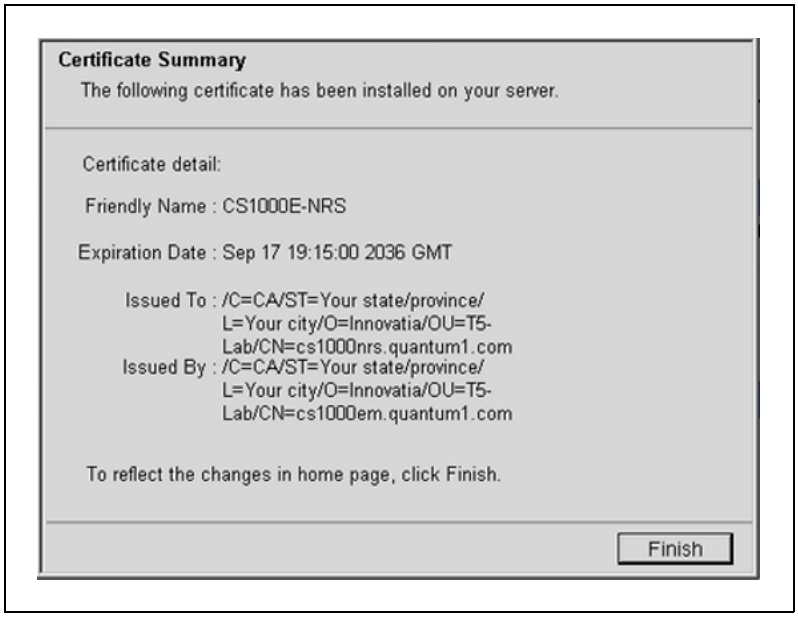
Figure 35
Certificate Request Summary



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

A **Certificate Summary** window appears with the certificate information, as shown in Figure 36 "Certificate Summary" (page 105).

Figure 36
Certificate Summary



10 Click **Finish**.

The status changes to signed.

11 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—End—

Create a certificate for SIP TLS signed by a trusted third-party 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 100 Release 5.0, see "Create a request for a third-party CA certificate for SIP TLS when upgrading the system" (page 109) 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 elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).

- 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 19 "Status types for certificate endpoints" (page 86).

Procedure 27

Creating a request for a certificate for SIP TLS 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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Certificates** pane, click the **Configure** button to the right of **SIP TLS**. The **Server Certificate** window appears, as shown in Figure 30 "Server Certificate window when no certificate is installed " (page 101).
5	Select **Create a new certificate request to be signed by third party** and click **Next**. The **Name and Security Settings** window appears, as shown in Figure 31 "Name and Security Settings" (page 101).
6	In the **Name and Security Settings** window, perform the following tasks: • In the **Friendly Name** field, enter a name. • From the **Bit Length** list, choose a bit length. The default value is 1024. • Click **Next**. The **Organization Information** window appears, as shown in Figure 32 "Organization Information" (page 102).
7	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, as shown in Figure 33 "Your Servers Common Name" (page 103).

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

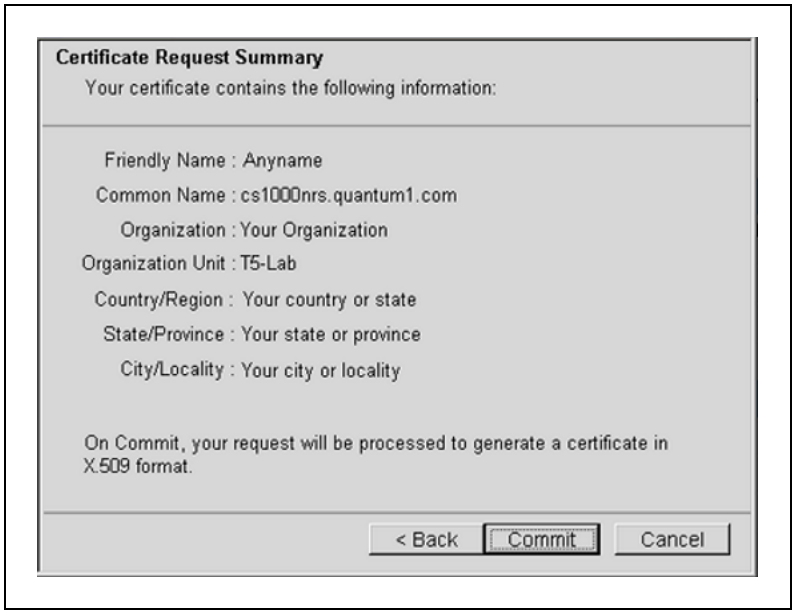
The **Geographical Information** window appears.

9 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, as shown in Figure 37 "Certificate Request Summary" (page 107).

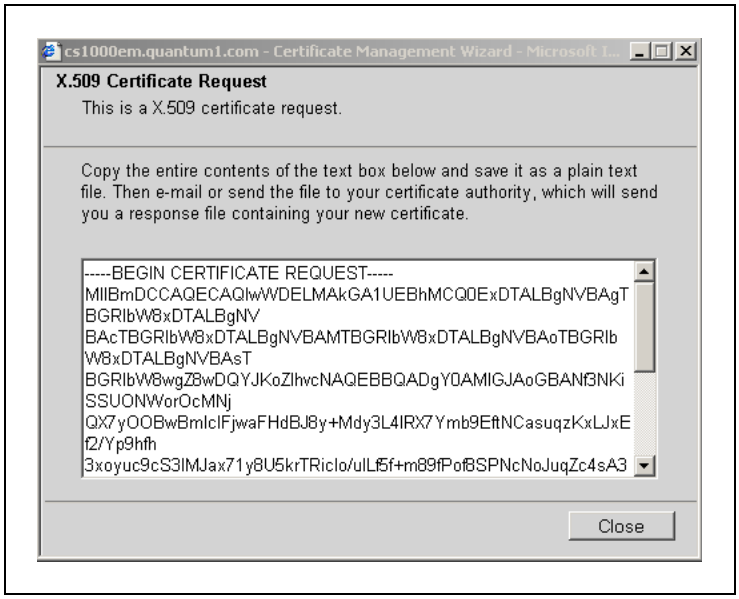
Figure 37
Certificate Request Summary



10 Click **Commit**.

The **X.509 Certificate Request** window appears, as shown in Figure 38 "X.509 Certificate Request" (page 108).

Figure 38
X.509 Certificate Request



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

11 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.

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

13 Click **Close**.

The status changes to pending.

14 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.

15 To process the pending request and install the certificate, follow the steps in Procedure 31 "Processing a pending certificate request by using ECM" (page 116).

The status changes to signed.

16 Follow the instructions from the third-party CA to download the certificates for the intermediate and root CAs.

17 Follow the steps in Procedure 19 "Adding a CA to an endpoint" (page 83) to add the intermediate CA to the server.

For more information about certificate chains, see Table 9 "Examples of certificates in a chain" (page 38).

18 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—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 5.0, the steps to install third-party CA-signed certificates vary depending on whether you request and install the certificate before upgrading, or after upgrading.

If you generate a certificate request and process the response for a third-party CA certificate after you upgrade the system, the certificate is not available immediately. It can take some time for the third-party CA to respond, and the amount of time can vary. Until the third-party CA signs and returns the CA, SIP TLS cannot function.

If you have already upgraded the system from CS 1000 Release 4.5 to CS 1000 Release 5.0, see Procedure 27 "Creating a request for a certificate for SIP TLS signed by third-party CA " (page 106). If you have not yet upgraded the system see Procedure 28 "Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading" (page 109) 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 28

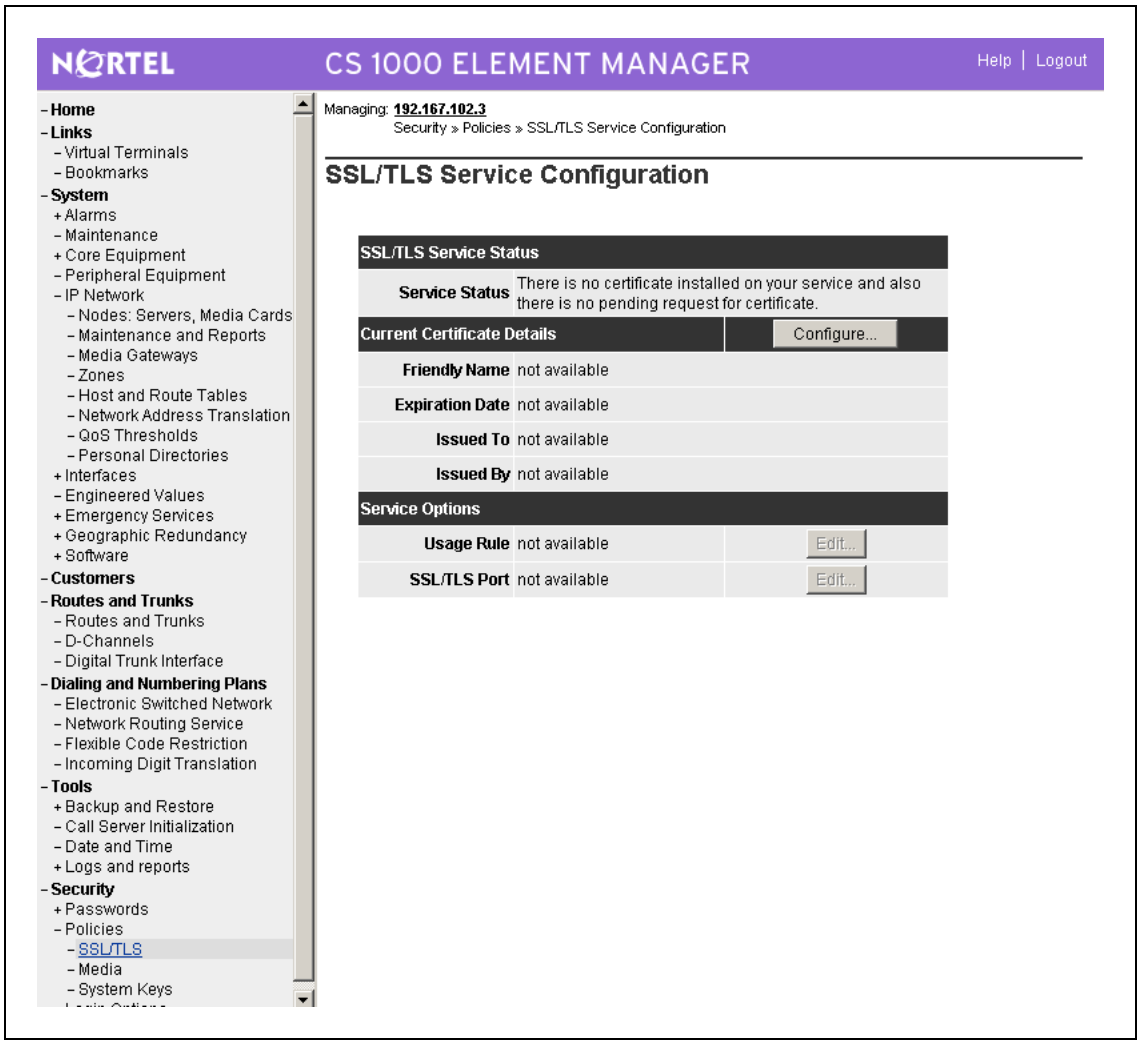
Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading

Step	Action
1	Before upgrading from CS 1000 4.5 to CS 1000 5.0, log on to Element Manager using an account that has SEC_ADMIN privilege.

2 Click **Security** > **SSL/TLS**.

The **SSL/TLS Service Configuration** page appears as shown in Figure 39 "SSL/TLS Service Configuration " (page 110).

Figure 39
SSL/TLS Service Configuration



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, as shown in Figure 31 "Name and Security Settings" (page 101).

6 Perform the following tasks:

- In the **Friendly Name** field, enter a name.
- From the **Bit Length** list, choose a bit length. The default value is 1024.
- Click **Next**.

The **Organization Information** window appears, as shown in Figure 32 "Organization Information" (page 102).

7 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, as shown in Figure 33 "Your Servers Common Name" (page 103).

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

The **Geographical Information** window appears.

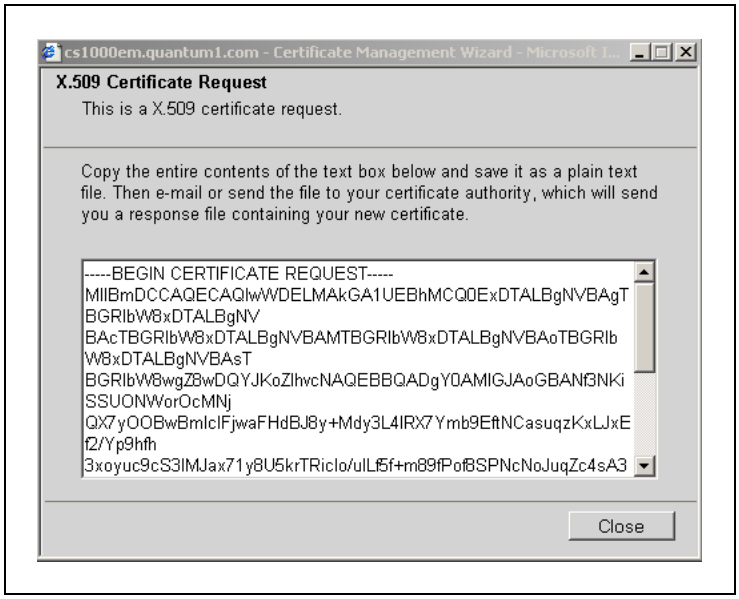
9 Perform the following tasks:

- 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.

10 The **X.509 Certificate Request** window appears, as shown in Figure 38 "X.509 Certificate Request" (page 108).

Figure 40
X.509 Certificate Request window



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

11 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.

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

13 Click **Close**.

The status changes to:
There is a pending new Certificate request on your service.

14 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 5.0, see Procedure 27 "Creating a request for a certificate for SIP TLS signed by third-party CA " (page 106)

Prerequisites

- 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 29
Processing a pending certificate response for SIP TLS when upgrading

Step	Action
1	Before upgrading from CS 1000 4.5 to CS 1000 5.0, log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security** > **SSL/TLS**. The **SSL/TLS Service Configuration** page appears as shown in Figure 39 "SSL/TLS Service Configuration " (page 110).
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 5.0
8	Follow the steps in Procedure 15 "Adding an element" (page 75) to add an element.
9	Follow the steps in Procedure 37 "Assigning an existing certificate by using ECM" (page 128) to assign the installed third-party CA certificate.
10	Use the steps in Procedure 19 "Adding a CA to an endpoint" (page 83) to add the certificate to the trusted CA list on each of the endpoints that must communicate with the element that owns this certificate.
11	Reboot the server that you changed in this procedure. The changes take effect only after the server reboots.

—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 elements; if the element to which you want to add a certificate is not yet configured, add it by following the steps in Procedure 15 "Adding an element" (page 75).
- 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 19 "Status types for certificate endpoints" (page 86).

Procedure 30

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Certificates** pane, click the **Configure** button to the right of **SIP TLS**. The **Server Certificate** window appears, as shown in Figure 30 "Server Certificate window when no certificate is installed " (page 101).
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, as shown in Figure 31 "Name and Security Settings" (page 101).
7	Enter a **Friendly Name** for the certificate.
8	Select a bit length from the **Bit length** list.
9	Click **Next**. The **Organization Information** window appears, as shown in Figure 32 "Organization Information" (page 102).

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, as shown in Figure 33 "Your Servers Common Name" (page 103).

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 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

19 Use the steps in Procedure 34 "Exporting the current self-signed certificate by using ECM" (page 121) to export the self-signed certificate.

20 Use the steps in Procedure 19 "Adding a CA to an endpoint" (page 83) 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 trusted third-party CA " (page 105). 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

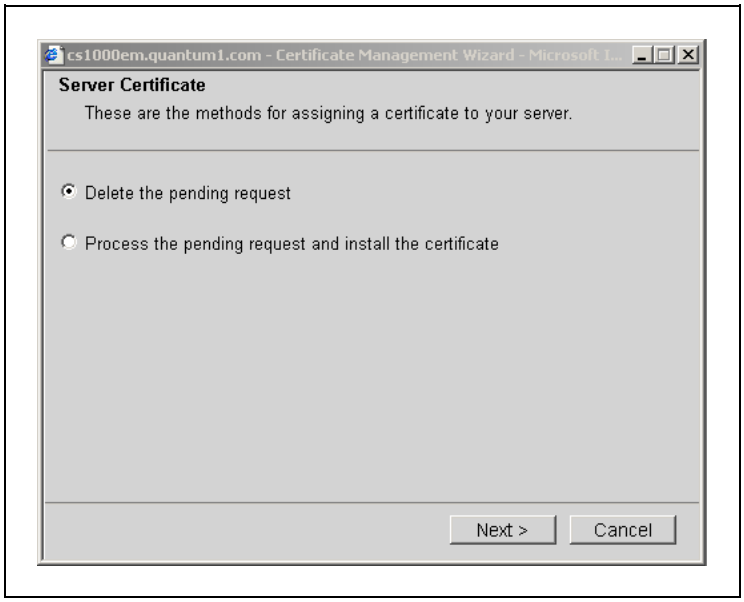
- Before you process a pending certificate request, ensure that the certificate endpoint status is pending or pending renew. For more information about certificate endpoint status types, see Table 19 "Status types for certificate endpoints" (page 86).

Procedure 31

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** pane, click **Configure**. The window appears, as shown in Figure 41 "Server Certificate window when a certificate is pending" (page 117).

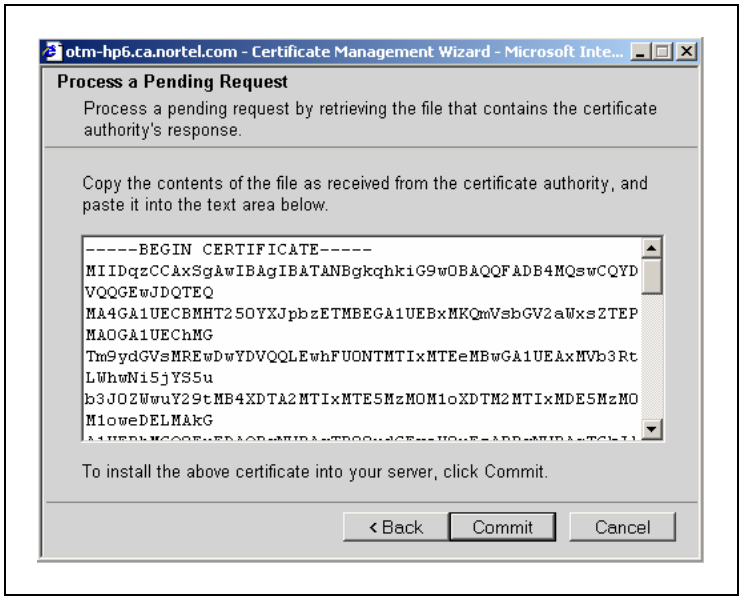
Figure 41
Server Certificate window when a certificate is pending



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

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

Figure 42
Process Pending Request window



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 19 "Status types for certificate endpoints" (page 86).

Procedure 32

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** section, click **Configure**. The **Server Certificate** window appears, as shown in Figure 41 "Server Certificate window when a certificate is pending" (page 117).
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

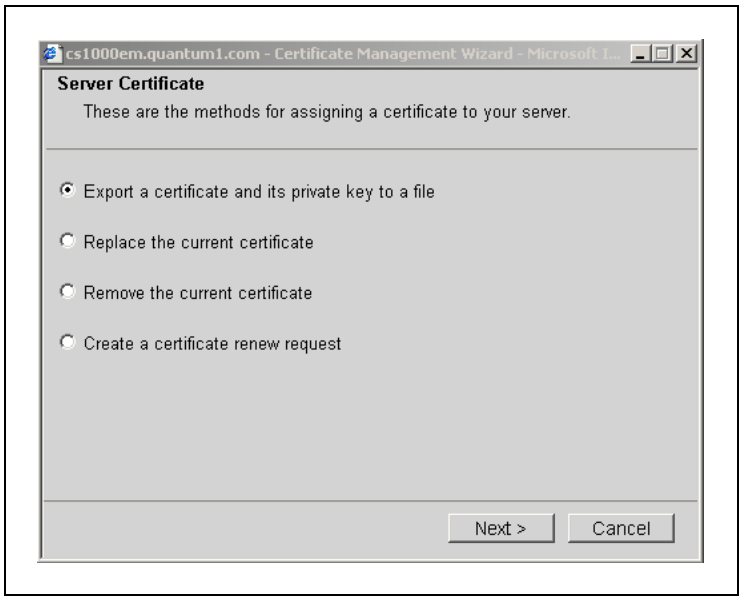
- Before you request a certificate renewal, ensure that the certificate endpoint status is signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 19 "Status types for certificate endpoints" (page 86).

Procedure 33

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** section, click **Configure**. The **Server Certificate** window appears, as shown in Figure 43 "Server certificate window when a signed certificate is installed" (page 120).

Figure 43
Server certificate window when a signed certificate is installed



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

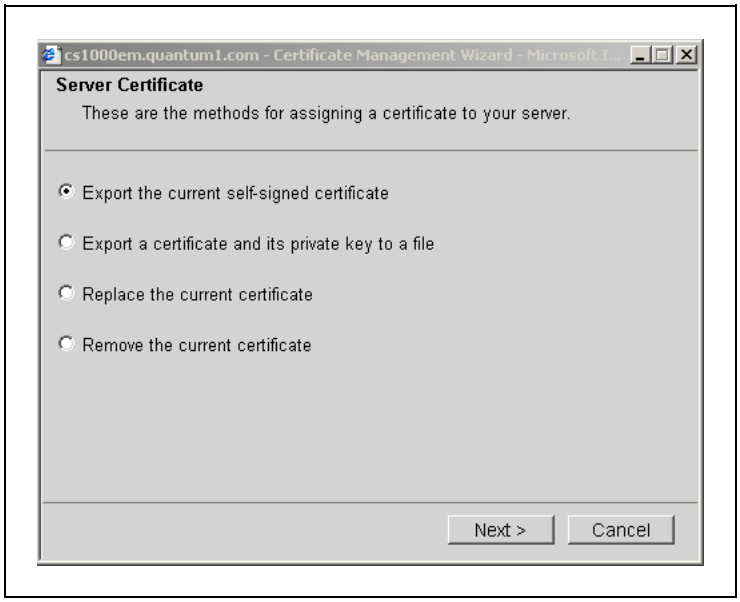
- Before you export the current self-signed certificate, ensure that the certificate endpoint status is self-signed. For more information about certificate endpoint status types, see Table 19 "Status types for certificate endpoints" (page 86).

Procedure 34

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Endpoint Details** pane, click **Configure** next to either **Web SSL** or **SIP TLS**. The **Server Certificate Configuration Wizard** window appears, as shown in Figure 44 "Server Certificate window when a self-signed certificate is installed" (page 122).

Figure 44
Server Certificate window when a self-signed certificate is installed



5 Select **Export the current 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 125).

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

Prerequisites

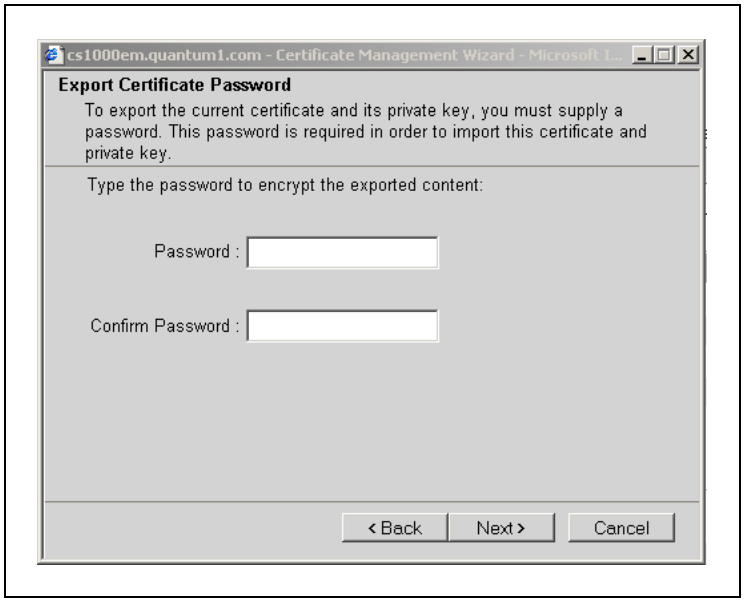
- Before you export the current certificate and its key, ensure that the certificate endpoint status is one of: self-signed, signed, about to expire, or expired. For more information about certificate endpoint status types, see Table 19 "Status types for certificate endpoints" (page 86).

Procedure 35

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, as shown in Figure 19 "Certificate Management " (page 87).
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, as shown in Figure 20 "Endpoint Details" (page 88).
4	Click the **Configure** button to the right of the **Web SSL** or **SIP TLS**. The **Server Certificate** window appears, as shown in Figure 43 "Server certificate window when a signed certificate is installed" (page 120) or Figure 44 "Server Certificate window when a self-signed certificate is installed" (page 122).
5	Select **Export the current certificate and its private key**, and click **Next**. The **Export Certificate Password** window appears, as shown in Figure 45 "Export Certificate Password" (page 124).

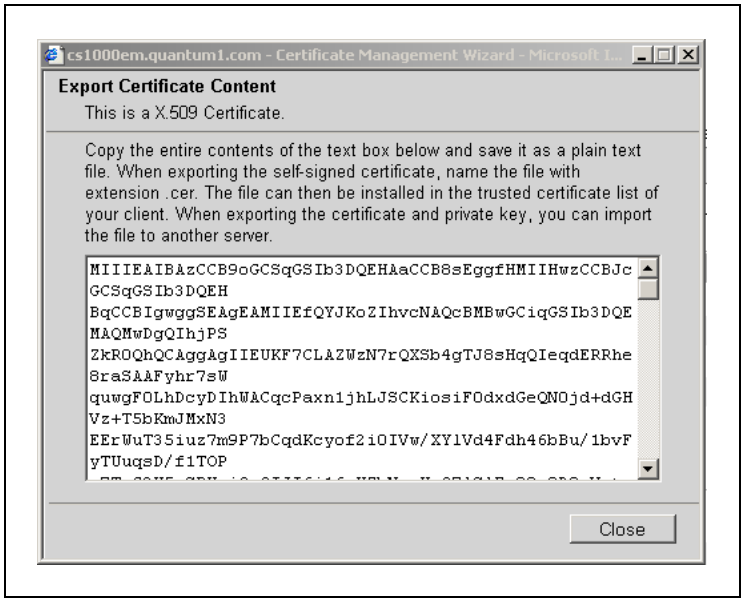
Figure 45
Export Certificate Password



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

The **Export Certificate Content** window appears, as shown in Figure 46 "Export Certificate Content" (page 124).

Figure 46
Export Certificate Content



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 122). 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 35 "Exporting the current certificate and its private key by using ECM" (page 123), 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 19 "Status types for certificate endpoints" (page 86).

Procedure 36

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

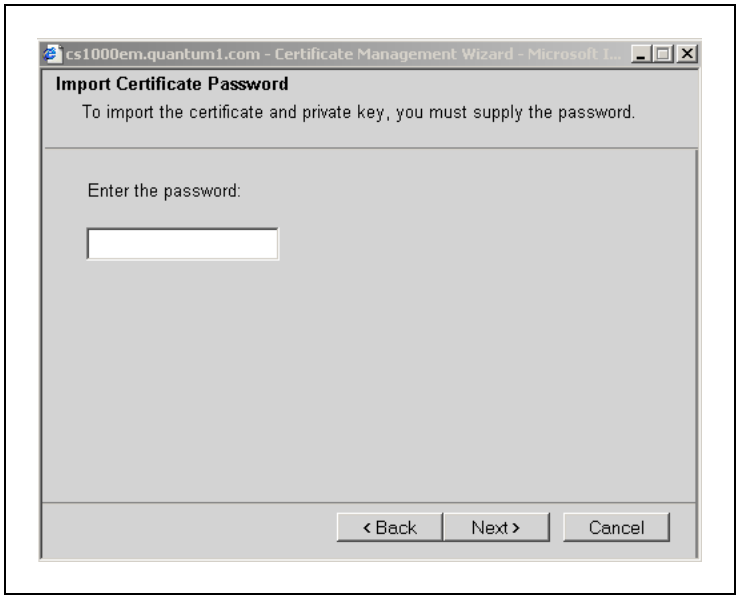
Step	Action
1	Log on to the ECM primary security server using an account that has SecurityAdministrator privilege.
2	Click **Security** > **Certificates**. The **Certificate Management** page appears, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint to which you want to import the certificate and key. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** section, click **Configure**.

The **Server Certificate** window appears, as shown in Figure 30 "Server Certificate window when no certificate is installed " (page 101).

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

The **Import Certificate Password** window appears, as shown in Figure 47 "Import Certificate Password" (page 126).

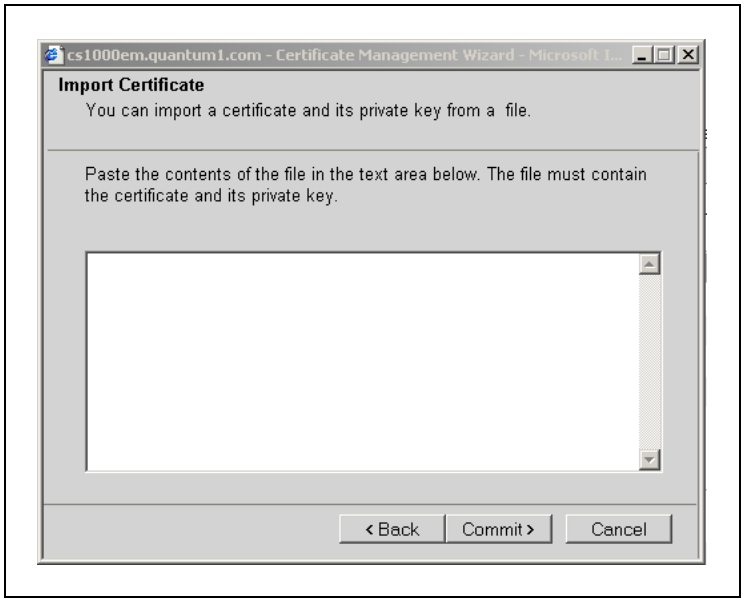
Figure 47
Import Certificate Password



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

The **Import Certificate** window appears as shown in Figure 48 "Import Certificate" (page 127).

Figure 48
Import Certificate



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 35 "Exporting the current certificate and its private key by using ECM" (page 123).

8 Click **Commit**.

The **Certificate Summary** window appears.

9 Click **Finish**.

10 Reboot the server that you changed in this procedure.

The changes take effect only after the server reboots.

—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 19 "Status types for certificate endpoints" (page 86).

Procedure 37
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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Endpoint Details** pane, click **Configure** next to either **Web SSL** or **SIP TLS**. The **Server Certificate** window appears, as shown in Figure 30 "Server Certificate window when no certificate is installed " (page 101).
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 **Next**. The **Certificate Summary** window appears.
7	Click **Finish**.
8	Reboot the server that you changed in this procedure. The changes take effect only after the server reboots.

—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 19 "Status types for certificate endpoints" (page 86).

Procedure 38

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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint that you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** section, click **Configure**. The **Server Certificate** window appears, as shown in Figure 43 "Server certificate window when a signed certificate is installed" (page 120) or Figure 44 "Server Certificate window when a self-signed certificate is installed" (page 122).
5	Select **Replace the current certificate**, and click **Next**. The **Available Certificate** window appears.
6	Select a certificate from the list, and click **Next**. The **Certificate Summary** window appears.
7	Click **Close**.

—End—

Remove the current certificate

Use the following procedure to remove the current certificate.

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 19 "Status types for certificate endpoints" (page 86).

Procedure 39
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, as shown in Figure 19 "Certificate Management " (page 87).
3	In the **Certificate Endpoints** pane, select the option button next to the endpoint you want to configure. The **Endpoint Details** pane appears, as shown in Figure 20 "Endpoint Details" (page 88).
4	In the **Web SSL** or **SIP TLS** section, click **Configure**. The **Server Certificate** window appears, as shown inFigure 43 "Server certificate window when a signed certificate is installed" (page 120) or Figure 44 "Server Certificate window when a self-signed certificate is installed" (page 122).
5	Select **Remove the current certificate**, and click **Next**. The **Remove a Certificate** window appears.
6	Click **Finish**.

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.

—End—

ISSS

This chapter contains procedures to help you protect system signaling. The chapter is divided into the following sections:

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

For more information about these features, see "Recommendations to protect confidentiality" (page 23).

About ISSS

ISSS provides a low level Intrasystem Signaling Security solution that works with all IP protocols, but does not apply to Small System Controller (SSC) based systems in Release 5.0. This section provides procedures to help you configure and use ISSS. For more information about ISSS, see "IPsec" (page 35).

ISSS configuration from the call server using overlays

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

Use the following procedure to change the system secret.

Procedure 40
Changing the system secret by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **CHG ISEC PSK**. A prompt appears that requests the new preshared key (PSK).
2	Enter the new PSK. The key must be 16-32 characters, and special characters (space, ~ ‘*@[]#) are not permitted. After you enter the new key, the system subjects it to strong password checking, and the strength of the PSK appears (Weak/Medium/Strong). If you are not satisfied with the strength of the entered key, return to step 1. A prompt appears, requesting confirmation of the new PSK.
3	Reenter the new PSK. The system sends a message to all connected devices indicating that the system secret has changed, and each device returns a message acknowledging that the new secret is received. After acknowledgement is received from all connected devices, the system saves the new secret locally.
4	After the connected devices acknowledge the change, complete any other ISSS configuration before proceeding to "Commit changes to ISSS configuration using overlays" (page 137).

—End—

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

Use the following procedure to configure the ISSS security option.

Procedure 41
Changing the ISSS option by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **CHG ISEC {OPTI|FUNC|FULL}** The system sends a message to all connected devices indicating the change.

2 After the connected devices acknowledge the change, complete any other ISSS configuration before proceeding to "Commit changes to ISSS configuration using overlays" (page 137).

—End—

For more information about the ISSS configuration options (OPTI, FUNC, FULL) for this feature, see Table 20 "Job aid: ISSS configuration options" (page 133).

Table 20
Job aid: ISSS configuration options

No Security	Intrasystem signaling security is disabled. Disabled is the default configuration.
Optimized Security	(Also called OPTI). Only the pbxLink and XMSG ports are encrypted using IPsec for a given IP address, and unencrypted traffic is permitted on all other ports. This applies to the Embedded Local Area Network (ELAN) ports only.
Functional Security	(Also called FUNC). All links between all known[1] elements are encrypted using IPsec (except SSH, SSL, AML, NTP). Unencrypted links from any other IP address are permitted.
Full Security	(Also called Standard Mode or FULL). All links between all known[1] elements are encrypted using IPsec (except SSH, SSL, AML, NTP). Links from any other IP address are encrypted using ISSS. If you configure ISSS to Full Security, Element Manager cannot operate over ELAN subnet unless you enable SSL.
[1] Known addresses are those IP addresses that are part of the node configured in Element Manager, or that are present in the list of trusted hosts.	

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

ATTENTION
To use Intrasystem Signaling Security (ISSS), you must upgrade all IP Media Gateways (IPMG) from SSC to Media Gateway Controller (MGC).

CAUTION
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 other devices can be disrupted. For more information about configuring IPsec on Linux, see Enterprise Common Manager Fundamentals (NN43001-116).

Procedure 42
Enabling ISSS by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **ENL ISEC** The system sends the updated status to all connected devices.
2	After the connected devices acknowledge the change, complete any other ISSS configuration before proceeding to "Commit changes to ISSS configuration using overlays" (page 137).

—End—

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

Procedure 43
Disabling ISSS by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **DIS ISEC** The system sends the updated status to all connected devices.
2	After the connected devices acknowledge the change, proceed to "Commit changes to ISSS configuration using overlays" (page 137).

—End—

Use the following procedure to view information about ISSS configuration.

Procedure 44
Viewing ISSS information by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **PRT ISEC {ALL | EXCEP | TARGET | SYNC}** For more information about the arguments for this command, see Table 21 "Job aid: arguments for PRT ISEC" (page 135).

—End—

Table 21
Job aid: arguments for PRT ISEC

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.

Configuring 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 manually only for devices that are not defined automatically, so do not create targets for:

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

Use the following procedure to manually create a target.

Procedure 45
Creating an ISSS target by using LD 117

Step	Action
1	At the LD 117 prompt, enter: **NEW ISECTAR <target IP>**.

—End—

Use the following procedure to enable a target.

Procedure 46
Enabling an ISSS target by using LD 117

Step	Action
1	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 disable a target.

Procedure 47
Disabling an ISSS target by using LD 117

Step	Action
1	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 manually delete a target.

Procedure 48
Deleting an ISSS target by using LD 117

Step	Action
1	At the LD 117 prompt, enter: `OUT ISECTAR <target IP>`.

—End—

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

Procedure 49
Viewing manually configured ISSS targets by using LD 117

Step	Action
1	Log on to the system using an account that has PWD2 privilege.
2	At the LD 117 prompt, enter: `PRT ISECTAR` to print the Intrasystem Signaling Security feature for a given target for the entire system.

—End—

Commit changes to ISSS configuration using overlays

ATTENTION

To add a new target after you have enabled and committed changes to ISSS configuration, you must either disable ISSS using Procedure 43 "Disabling ISSS by using LD 117" (page 134), or use the ISSS management tools at the OAM prompt, as described in "Manual ISSS configuration on each device" (page 137).

Procedure 50

Committing changes to ISSS configuration by using LD 117

Step	Action

1	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])`

2	Enter either: **yes** to commit changes **OR** **no** to cancel

—End—

Manual ISSS configuration on each device

Use the commands described in the following procedures to configure ISSS settings on individual devices by using the command line interface (CLI).

Procedure 51
Changing the system secret on the local device by using CLI

Step	Action
1	Log on to the OAM/PDT/IPL shell.

2	Enter the command **isecChgPSK**.
	The following message appears:
	`oam> isecChgPSK`
	`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]):`

3	Enter the new PSK. The key must be 16-32 characters, and special characters (space, ~ '*@[]#) are not permitted. A prompt appears that requests confirmation of the new PSK.
4	Reenter the new PSK. The device saves the secret.

—End—

Procedure 52
Changing the Intrasystem Signaling Security option by using CLI

Step	Action
1	Log on to the OAM/PDT/IPL shell.

2	Enter the command **isecChgLevel**.
	The following message appears:
	`oam> isecChgLevel`
	`isecChgLevel [OPTI/FUNC/FULL]`
	`Change ISEC security level locally.`
	`oam> isecChgLevel opti`
	`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]):
```

3 Enter either:

yes

OR

no

—End—

Configuring ISSS targets on a local device

ISSS is automatically enabled on the following devices:

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

Use the following procedure to manually create an ISSS target for devices such as CallPilot or Enterprise Common Manager (ECM), so that those devices can encrypt traffic using ISSS.

Procedure 53
Creating a new ISSS target on a local device by using CLI

Step	Action
1	Log on to OAM/PDT/IPL shell.

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? (Yes/[No]):yes`

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

3 Enter either:

yes to save the new target locally

OR

no

—End—

Use the following procedure to enable an ISSS target for devices such as CallPilot or Enterprise Common Manager (ECM).

Procedure 54
Enabling an ISSS target on a local device by using CLI

Step	Action
1	Log on to OAM/PDT/IPL shell.
2	Enter the command **isecEnlTarget <IP ADDRESS>**.

ATTENTION

This command returns an error in either of the following cases:

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

A warning message appears, as well as a prompt that requests confirmation.

3 Enter either:

yes to save the new target security status locally

OR

no

—End—

Use the following procedure to disable an ISSS target for devices such as CallPilot or Enterprise Common Manager (ECM).

Procedure 55
Disabling an ISSS target on a local device by using CLI

Step	Action
1	Log on to OAM/PDT/IPL shell.
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? (Yes/[No]):yes` `The target has been disabled.`
3	Enter either: **yes** to save the new target security status locally **OR** **no**

—End—

Use the following procedure to delete an ISSS target for devices such as CallPilot or Enterprise Common Manager (ECM).

Procedure 56
Deleting an ISSS target on a local device by using CLI

Step	Action
1	Log on to OAM/PDT/IPL shell.

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?  (Yes/[No]):yes
The target has been deleted locally.
```

3 Enter either:

yes to remove the target locally

OR

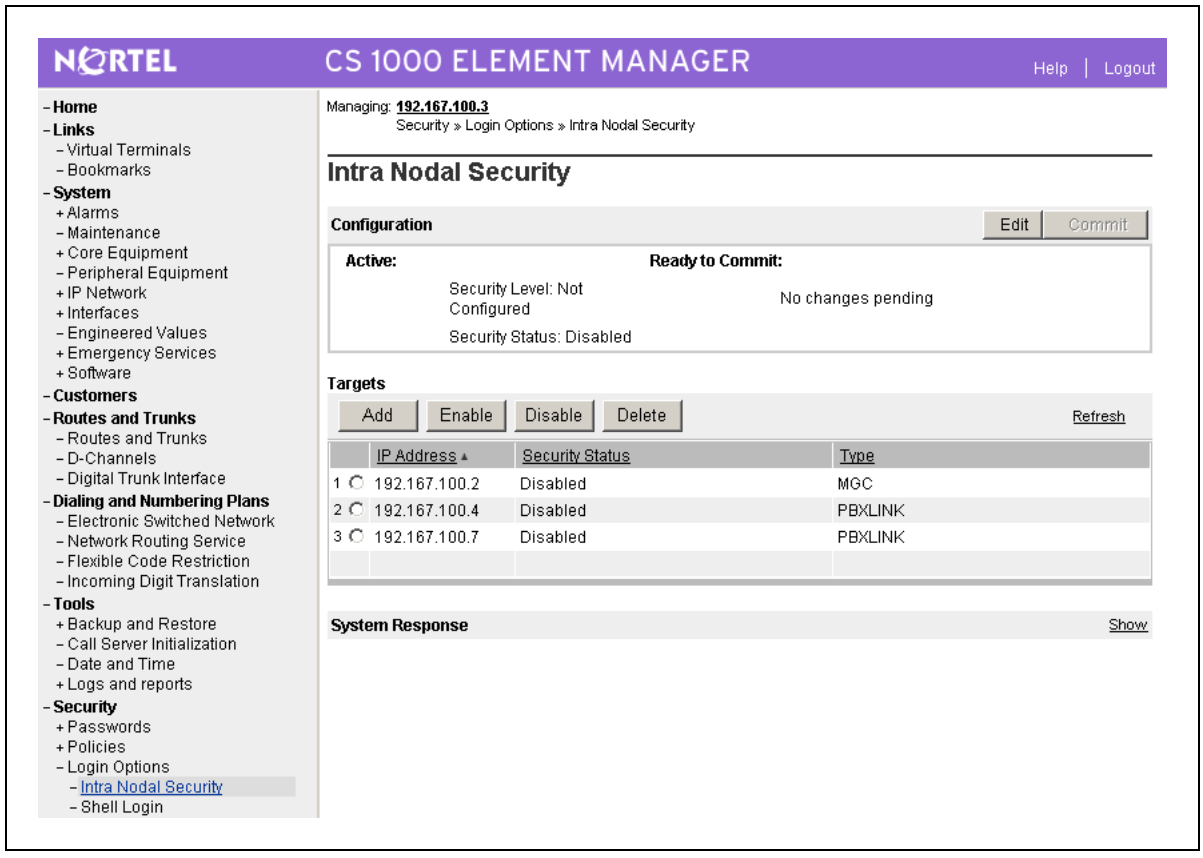
no

—End—

ISSS configuration using Element Manager

In Element Manager, you can use the Intra Nodal Security page, as shown Figure 49 "Intra Nodal Security in Element Manager" (page 142), to configure Intrasystem Signaling Security.

Figure 49
Intra Nodal Security in Element Manager

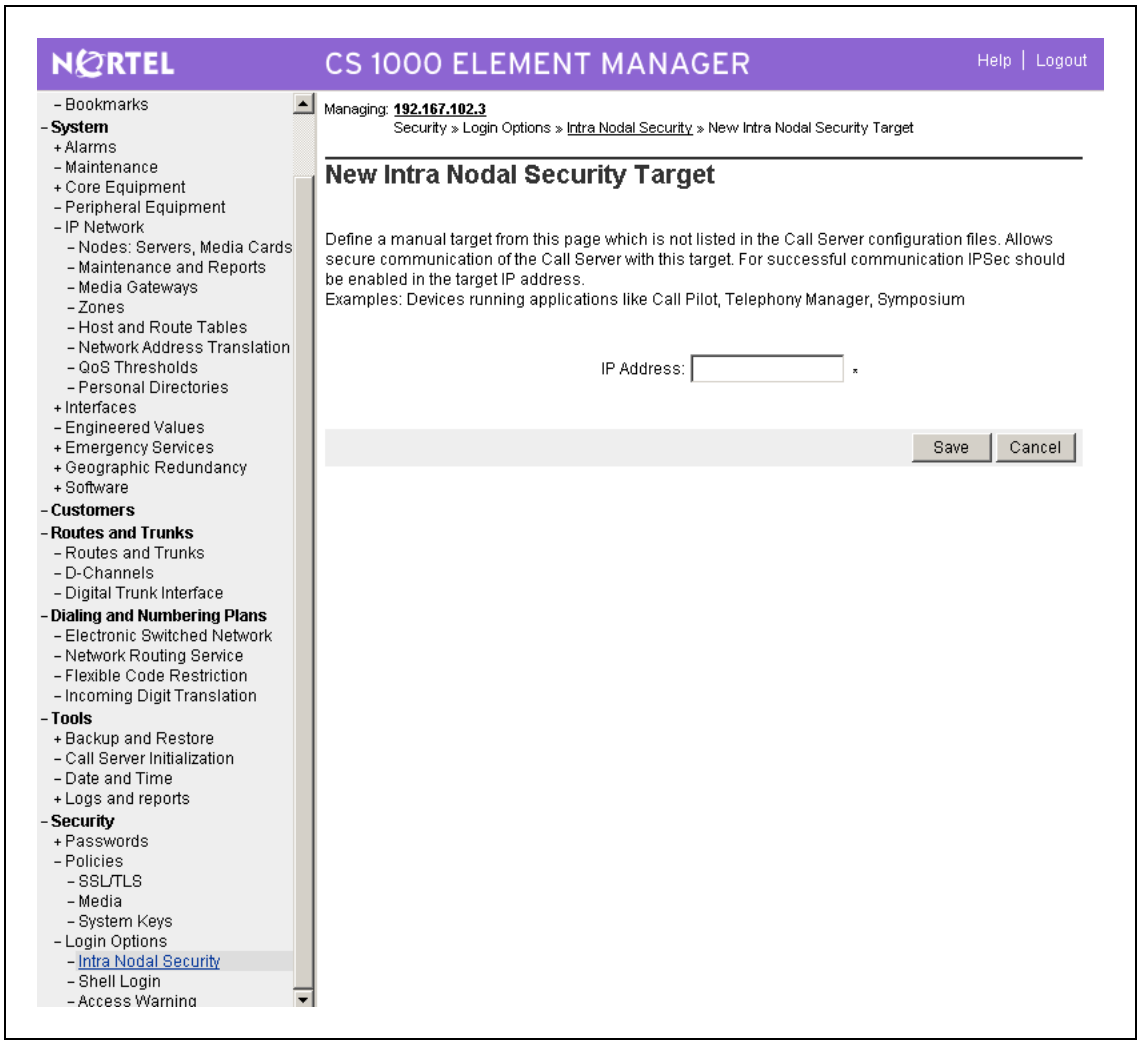


Use the following procedure to add a target manually in Element Manager.

Procedure 57
Adding an ISSS target manually by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Login Options > Intra Nodal Security** . The **Intra Nodal Security** page appears, as shown in Figure 49 "Intra Nodal Security in Element Manager" (page 142).
3	Click **Add**. The **New Intra Nodal Security Target** page appears, as shown in Figure 50 "New Intra Nodal Security Target " (page 144).

Figure 50
New Intra Nodal Security Target



4 Enter the IP Address for the new target.

5 Either:

Click **Save** to save the changes and return to the Intra Nodal Security page.

OR

Click **Cancel** to discard your changes and return to the Intra nodal security page.

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

—End—

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

Procedure 58
Editing an existing ISSS target by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Login Options > Intra Nodal Security** . The **Intra Nodal Security** page appears, as shown in Figure 49 "Intra Nodal Security in Element Manager" (page 142).
3	Select the option button next to the entry you want to edit.
4	Either: Click **Enable** **OR** Click **Disable** **OR** Click **Delete** A confirmation requester appears.
5	Either: Click **OK** **OR** Click **Cancel** to discard your changes and return to the Intra nodal security page.
6	Click **Commit** to commit your changes to the system.

—End—

Use the following procedure to delete an ISSS target.

Procedure 59
Deleting an ISSS target by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.

2 Click **Security > Login Options > Intra Nodal Security** .

The **Intra Nodal Security** page appears, as shown in Figure 49 "Intra Nodal Security in Element Manager" (page 142).

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

4 Click **Delete**.

A confirmation requester appears.

5 Either:

Click **OK** to delete the target.

OR

Click **Cancel** to discard your changes.

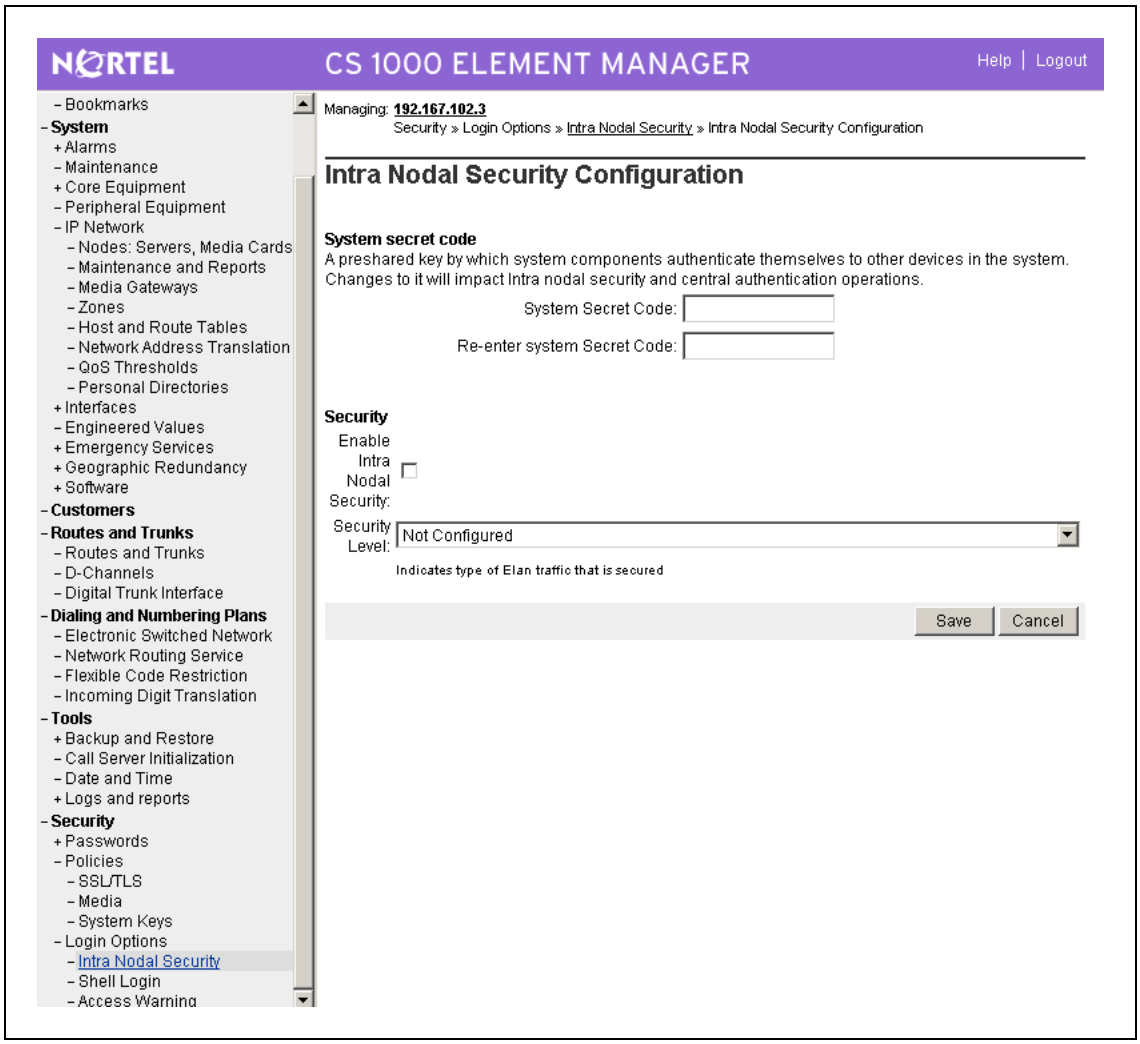
—End—

Use the following procedure to configure ISSS options, to change the security status, or to change the System Secret Code.

Procedure 60
Configuring ISSS options by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Login Options > Intra Nodal Security** . The **Intra Nodal Security** page appears, as shown in Figure 49 "Intra Nodal Security in Element Manager" (page 142).
3	Click **Edit**. The **Intra Nodal Security Configuration** page appears, as shown in Figure 51 "Intra Nodal Security Configuration " (page 147).

Figure 51
Intra Nodal Security Configuration



4 Configure any or all of the following options:

- Enter a new system secret **System Secret Code** field, and reenter it in the **Re-enter system Secret Code** to confirm the new value.
- Select or clear the **Security Status** option box.
- From the **Security Level** menu, choose one of **Optimized**, **Functional** or **Full**.

5 Either:

Click **Save**

OR

Click **Cancel**

The Intra Nodal Security page appears.

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

—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:

For more information about user and password management concepts in Communication Server 1000 (CS 1000) Release 5.0, see "User and password management concepts" (page 39).

ATTENTION

To configure or access many security features, including many user management features, you must log on with an account that has SEC_ADMIN privilege. The SEC_ADMIN privilege is available to Level 2 (PWD2) user accounts that are configured with the authority to administer accounts.

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.

Roles and privileges

User account information is stored in the file acct_002.db, while information about the privileges assigned to each user is stored in the file roles.db.

When you add a user or change a password, the system automatically schedules an EDD to update the acct_002.db and roles.db files on each local device. When an EDD occurs, the system distributes the updated acct_002.db and roles.db 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 200).

The roles.db file always contains, at minimum, two accounts:

- an account that has PWD2 access
- an account that has PDT2 access

Customer passwords

For each Customer Number defined on the system, you can assign a Secure Data Password and an Attendant Administrative Access Code.

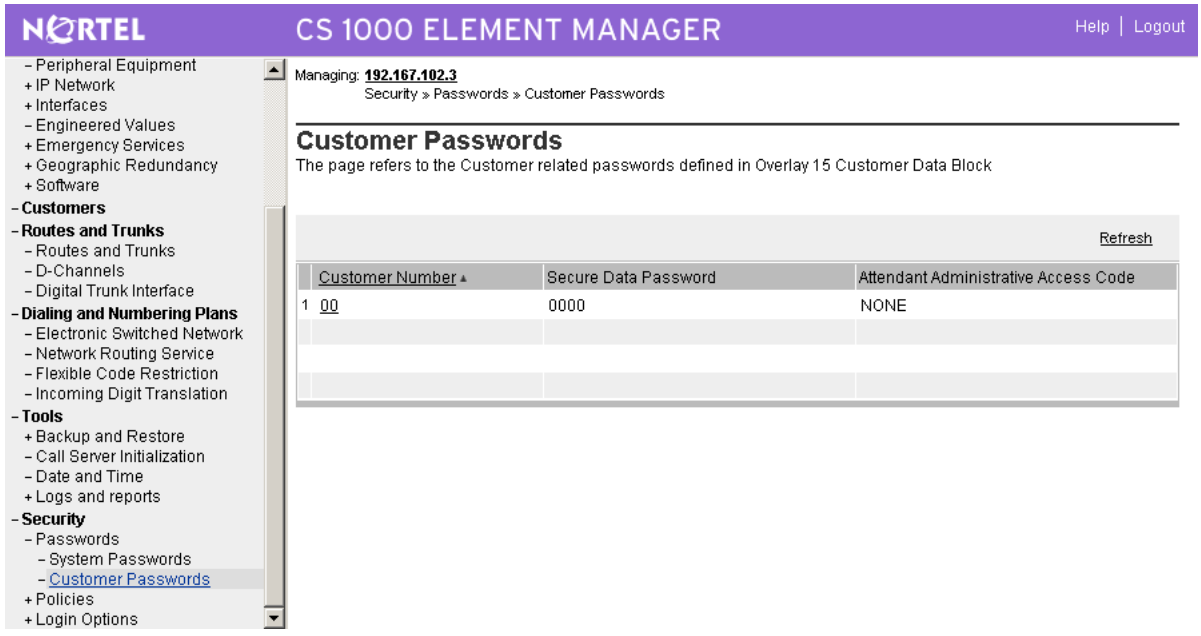
Use the following procedure to assign or change the Secure Data Password or Attendant Administrative Access Code.

Procedure 61

Assigning or changing customer passwords

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Customer Passwords** . The **Customer Passwords** page appears, as shown in Figure 52 "Customer Passwords" (page 151).

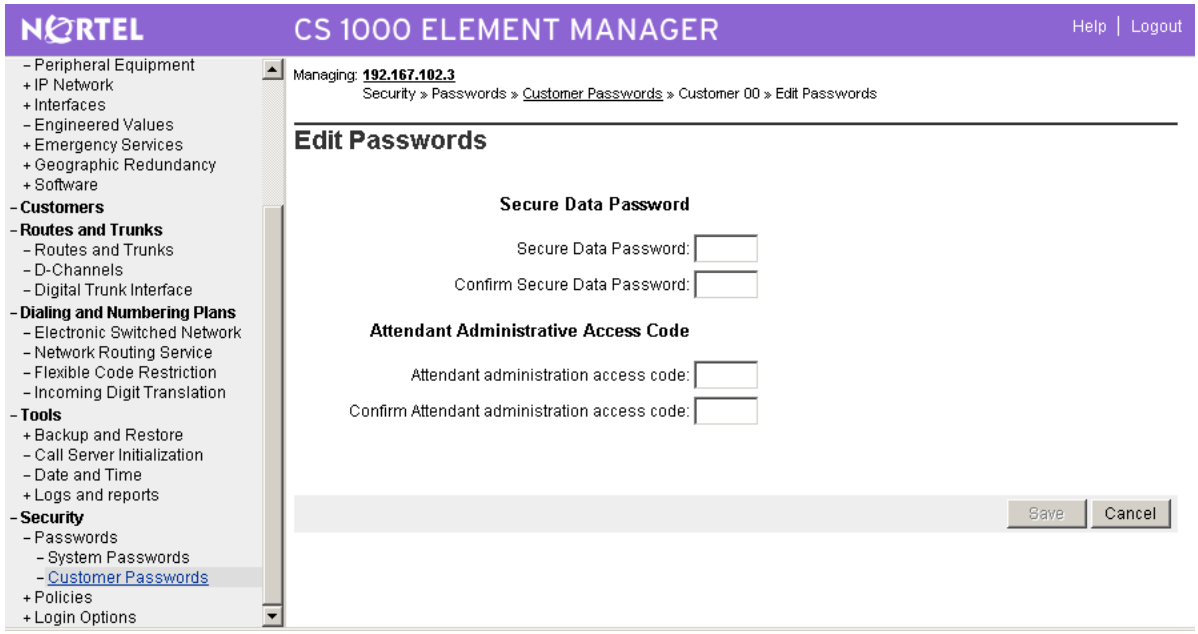
Figure 52
Customer Passwords



3 Click a Customer Number.

The **Edit Passwords** page appears, as shown in Figure 53 "Edit Passwords" (page 152).

Figure 53
Edit Passwords



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 Either:

Click **Save**

OR

Click **Cancel**

The **Customer Passwords** 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. The sequence of prompts for LD 17 is shown in Table 22 "Job aid: LD 17 user and password prompts" (page 153).

Table 22
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 24 "Job aid: Password restrictions" (page 163).
NEW_PASSWORD	a...a	New password. For password requirements, see Table 24 "Job aid: Password restrictions" (page 163).
CONFIRM	a...a	Confirm the new password
ACCT	(NO) YES	Administer accounts. This prompt only appears when adding or modifying 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)*.

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.

Procedure 62

Adding a user other than LAPW by using LD 17

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
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 **`<aaa>`**, where <aaa> is the type of account to create. For more information, see Table 22 "Job aid: LD 17 user and password prompts" (page 153). If you are creating an LAPW user, see "Add an LAPW user" (page 155).
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. For information about the restrictions on LAPW user names and passwords, see Table 24 "Job aid: Password restrictions" (page 163).
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—

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:

Procedure 63
Adding an LAPW (Overlay) user by using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 23 "Job aid: Restrictions on LAPW users and passwords" (page 158) 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 24 "Job aid: Password restrictions" (page 163) 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 **<xx> TEN <yy>**, to specify the customers the user has access to, where <xx> is the customer number, and <yy> is the tenant number.

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 **<xx>**, where xx are the password options permitted for password PWnn.

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—

Use the following procedure to create an LAPW user with Set Based Administration access:

Procedure 64
Adding an LAPW (Set Based Administration) user by using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 23 "Job aid: Restrictions on LAPW users and passwords" (page 158) 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 **<custnum> TEN <tennum>**, to specify the customers the user can access, where <custnum> is the customer number, and <tennum> is the tenant number.
12	At the LD 17 OPT prompt, enter **<value>**, where <value> are the password options permitted for password PWnn.

For more information about the password options that you can enter at the OPT prompt, see Software Input Output Administration (NN43001-611).

—End—

Table 23
Job aid: Restrictions on LAPW users 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.

Use the following procedure to view information about LAPW user accounts.

Procedure 65
Viewing LAPW user information by using LD 22

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
2	At the LD 22 `REQ` prompt, enter **`PRT`**.
3	At the LD 22 `TYPE` prompt, enter **`PWD`** to view user information.

—End—

For more information about LAPW and the prompts in LD 17 and LD 22, see *Software Input Output Administration (NN43001-611)*.

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.

Procedure 66
Configuring the LAPW Audit Trail by using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.

2 At the LD 17 REQ prompt, enter **CHG**.

3 At the LD 17 CHG 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 22 "Job aid: LD 17 user and password prompts" (page 153).

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 **<value>**, where <value> is the word size for the Audit Trail file, in the range of 50–1500. The default value is 50.

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—

Use the following procedure to access information stored in the Audit Trail.

Procedure 67
Viewing information stored in the LAPW Audit Trail by using LD 22

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 68
Deleting a user by using LD 17

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
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 22 "Job aid: LD 17 user and password prompts" (page 153).

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.

Procedure 69
Changing a password by using LD 17

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
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).

Procedure 70
Changing your PDT password by using the CLI

Step	Action
1	Log on to the PDT prompt.
2	Enter the command **passwd**.
3	Enter your existing password.
4	Enter the new password. The new password must be different from the current password.
5	Reenter the new password. A confirmation message appears.

—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 200).

Use the following procedure to view information about user accounts.

Procedure 71
Viewing account information by using LD 22

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
2	At the LD 22 REQ prompt, enter **prt**.
3	At the LD 22 TYPE prompt, enter **pwd**. Details of all accounts appear.

—End—

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 43). For recommendations about what password settings to use, see "Recommended password management practices" (page 21).

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 72

Configuring password settings by using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 22 "Job aid: LD 17 user and password prompts" (page 153).
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 24 "Job aid: Password restrictions" (page 163).
5	At the LD 17 `FPC` prompt, enter **`YES`** to enable Force Password Change. 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 **`<value>`** to enable Inactive Session Timeout. Where <value> is the number (in the range 1–1440) of minutes of inactivity before a session ends automatically.
7	At the LD 17 `FLTH` prompt, enter **`<value>`** to enable Failed Log in Threshold. Where <value> is the number (in the range 0–9) of

times a user can successively fail to log on before their account is locked out.

8 At the LD 17 LOCK prompt, enter **<value>** to configure the Lockout time. Where <value> is the number (in the range 0–270) of minutes an account remains locked after the Failed Log in Threshold is reached.

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 **<value>** to configure the word size of Audit Trail buffer. Where <value> is a number in the range 50–1500.

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 24
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.

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 73
Resetting call server passwords by using the CLI

Step	Action
1	At the call server prompt, press **Ctrl+p Ctrl+d Ctrl+t** to enable PDT mode on the call server. A prompt appears, requesting a user name.

2	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`

3	Enter either: **QUIT** to exit without resetting any passwords, **OR** **<user>**, where <user> is a PWD2 level 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.
4	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.

5 Press **Enter**.

6 Enter the new PWD2 password.

7 Reenter the new PWD2 password.

8 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 200).

—End—

Password reset for other devices

Use the information in Table 25 "Password reset for other system devices and applications" (page 165) to reset the passwords for system devices or applications other than the call server.

Table 25
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)*.

Check for Insecure passwords

Use the following procedure to display detailed information about user that have insecure passwords. Passwords are not displayed.

Procedure 74
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—

"IPWD output" (page 168) shows an example of the output form the PRT IPWD command.

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
```

View all user accounts

Use the following procedure to display detailed information about all user accounts. Passwords are not displayed.

Procedure 75

Viewing all user accounts by using LD 22

Step	Action
1	At the LD 22 REQ prompt, enter **PRT**.
2	At the LD 22 TYPE prompt, enter **PWD**.

—End—

"Example output from the PRT PWD command" (page 168) shows an example of the output from the PRT PWD command.

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)
OVL    001   002   003   004   005   006   007   008   009   010
A
       011   012   013   014   015   016   017   018   019   020
       021   022   023   024   025   026   027   028   029   030
       031   032   033   034   035   036   037   038   039   040
       041   042   043   044   045   046   047   048   049   050
       051   052   053   054   055   056   057   058   029   060
       061   062   063   064   065   066   067   068   069   070
       071   073   073   074   075   076   077   078   079   080
       081   082   083   084   085   086   087   088   089   090
       091   092   093   094   095   096   097   098   099   117
       135   137   143
CUST
HOST NO
MAT NO
OPT PSCA RBBD CFPA LLCD PROD LOSD FORCD MOND

USER_NAME LAPW3 **INSECURE**
TYPE LAPW_OVL
OVLA 017 022
CUST
HOST NO
MAT NO
OPT PSCA RDBD DFPA LLCD PROD LOSE FORCD MOND

USER_NAME SBA2
PWTP SBA
LEVL ADMN
CUST
OPT FEAD NAMA TADD TOLD DTD TRKD INSD
```

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 26 "User administration commands" (page 170).

Table 26
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 privilege management using overlays

Use the following procedure to assign user privileges.

Procedure 76
Assigning privileges using LD 17

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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**.
5	Either: Assign privileges to a role by entering **`NEW`** at the `ACCOUNT_REQ` prompt. A new account is created, and a new role is defined based on the account type you select for the new account. The roles.mem and acct_002.mem files are updated with the new role. **OR** Modify a role by entering the CHG command at the ACCOUNT_REQ prompt. Edit the account settings and password. You cannot use this method to change an account type; to do so, you must delete

and recreate the user. The roles.mem and acct_002.mem files are updated with the new role.
OR
Delete a role by deleting the user associated with it. Enter the OUT command at the ACCOUNT_REQ prompt. The roles.mem and acct_002.mem files are updated.

—End—

When an EDD is performed, the updated acct_002.mem and roles.mem files overwrite the acct_002.db and roles.db files, and are distributed to all Voice Gateway Media Card, MGC, and IPMG devices. To force an immediate EDD, see "Force an EDD using overlays" (page 200).

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 SEC_ADMIN privilege can change their own password only.

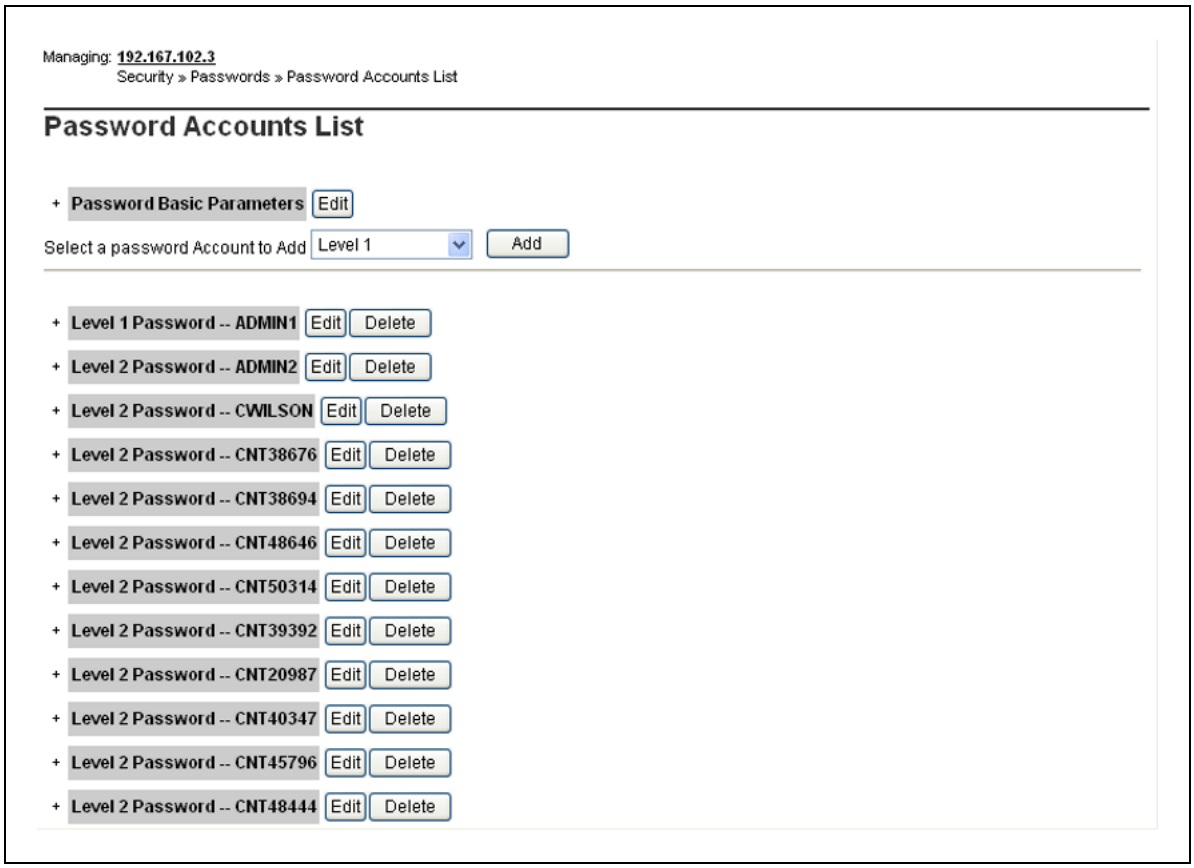
Add a user

Use the following two procedures to add user accounts.

Procedure 77
Adding a user other than LAPW by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears, as shown in Figure 54 "Password Accounts List" (page 172).

Figure 54
Password Accounts List

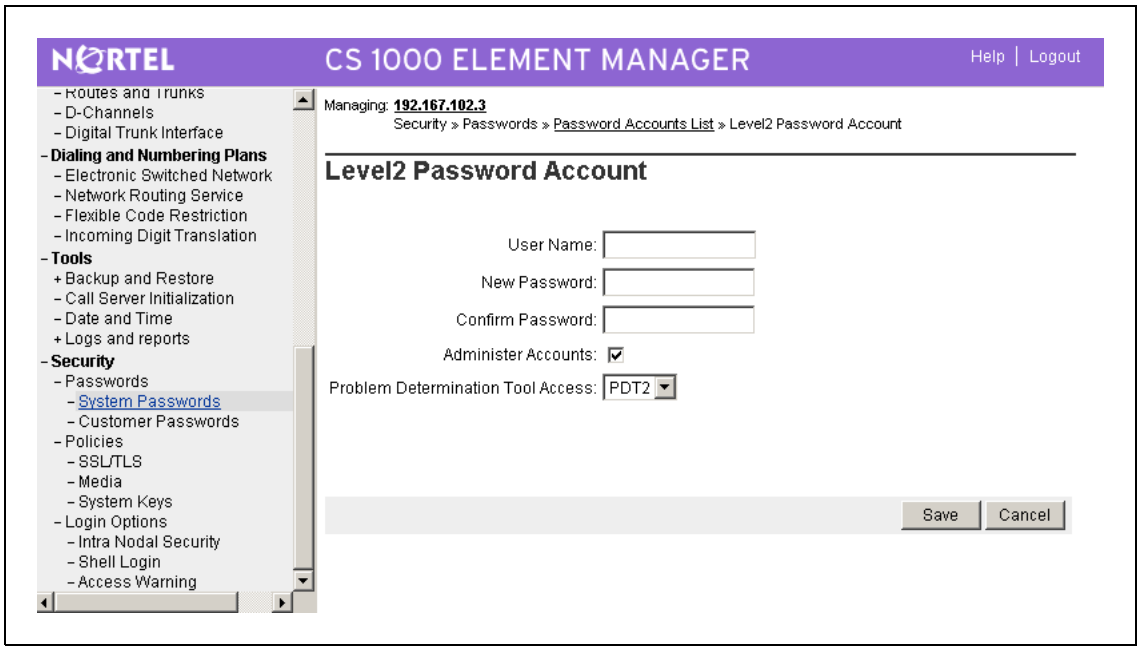


3 From the **Select a password Account to Add** list, select one of the listed account types. For more information about the account types available, see "System accounts" (page 40).

4 Click **Add**.

The **Password Account** page appears, as shown in Figure 54 "Password Accounts List" (page 172). The page varies slightly depending on what type of account you selected.

Figure 55
Password Account



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 Either:

Click **Save** to save the new user, and return to the **Password Accounts List** page.

OR

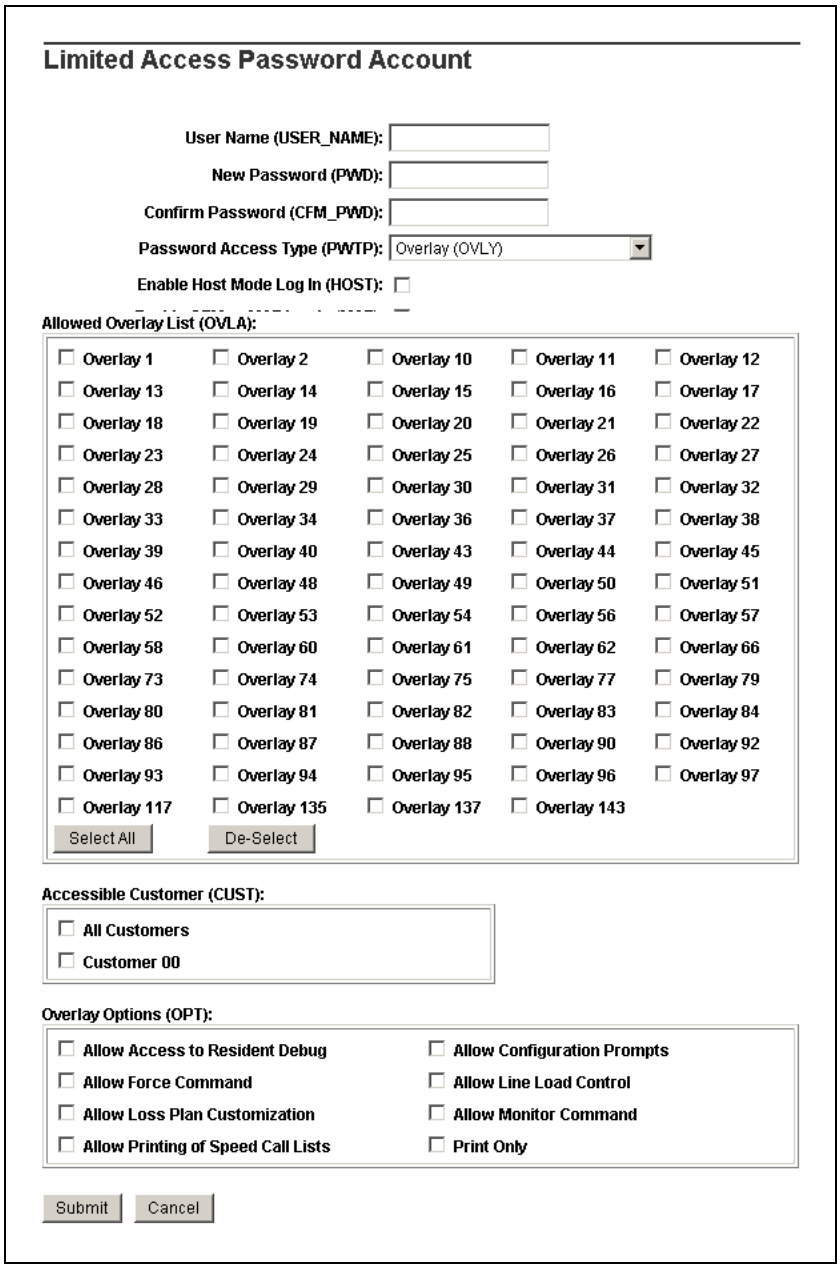
Click **Cancel** to cancel the changes, and return to the **Password Accounts List** page.

—End—

Procedure 78
Adding an LAPW user by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears, as shown in Figure 54 "Password Accounts List" (page 172).
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 40).
4	Click **Add**. The **Limited Access Password Account** page appears, as shown in Figure 56 "Limited Access Password Account " (page 175).

Figure 56
Limited Access Password Account



5 Enter the user name in the **User name** field, and the password in the **New password** and **Confirm password** fields.

6 Configure the following values:

- In the **Password access type** list, choose either **Overlay (OVLY)** or **Set Based Administration (SBA)**.
- Select or clear **Enable host mode log in**.

- Select or clear **Enable OTM or MAT Log In (MAT_READ_ONLY):**
- In the **Problem Determination Tool Access (PDT)** list, choose one of **NO**, **PDT1** or **PDT2**.
- Select or clear **Restrict MAT Write Access (MAT_READ_ONLY):**
- 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.
- Select or clear the various customers in the **Accessible Customer (CUST)** list.
- Select or clear the various options in the **Overlay Options (OPT)** list.

7 Either:

Click **Save** or **Submit** to save the new user, and return to the **Password Accounts List** page.

OR

Click **Cancel** to cancel the changes, 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 Level 1 and Level 2 passwords, you must log on using an account that has Level 2 access.

Procedure 79
Editing an existing user by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears, as shown in Figure 54 "Password Accounts List" (page 172).
3	Next to the account you want to modify, click **Edit**.

The **Password Account** page appears, as shown in Figure 55 "Password Account" (page 173) or Figure 56 "Limited Access Password Account " (page 175).

Make changes to the password and access capabilities of the selected user by editing the fields and selecting or clearing the various options.

4 Either:

Click **Save** or **Submit** to save your changes and return to the **Password Accounts List** page.

OR

Click **Cancel** to cancel the 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 Network Routing Service

Level 2 (PWD2) users manage accounts and passwords on the stand-alone Signaling Server running Network Routing Service (NRS). The Level 2 (PWD2) user can issue commands from the OAM shell as shown in Table 27 "Commands issued to manage accounts and passwords on the stand-alone NRS" (page 177).

Table 27
Commands issued to manage accounts and passwords on the stand-alone NRS

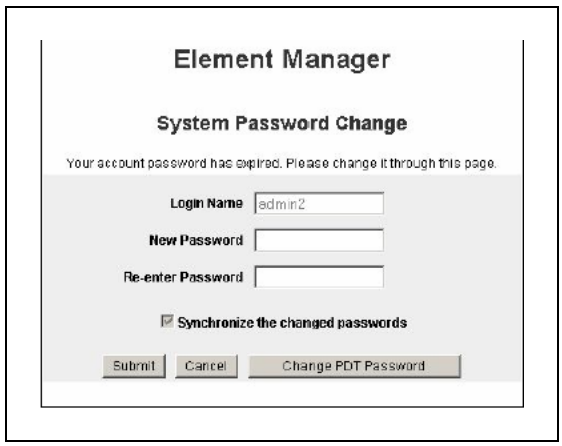
Command	Description
adminUserPassword Change [userID]	Use this command to give users the ability to change their own password, or to give a Level 2 (PWD2) user the ability to change any user password specified in the userID field. Requires Level 2 (PWD2) access.
adminUserCreate [userID]	Use this command to create an account specified in the userID field. Requires Level 2 (PWD2) access.

Command	Description
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 57 "System password change" (page 178).

Figure 57
System password change



Edit global password settings

Use the following procedure to configure settings that apply to all accounts.

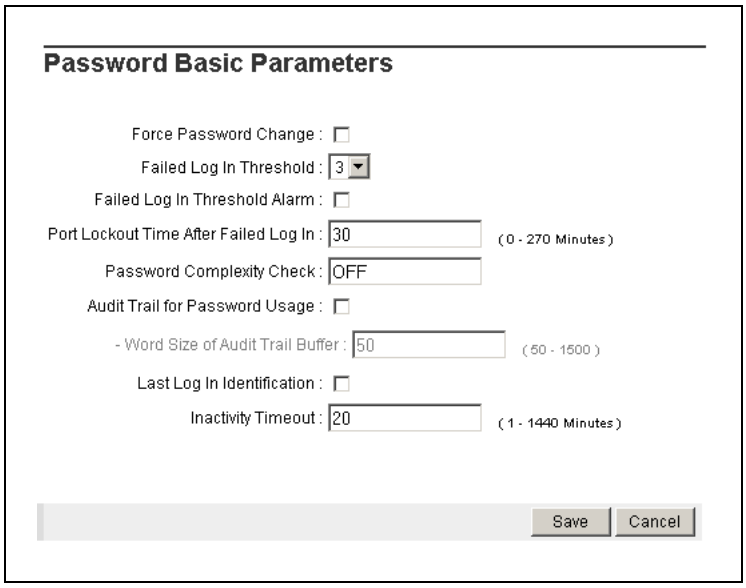
For more information about the features described in this section, see "Global password settings" (page 43).

Procedure 80
Editing global password settings by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Passwords > System Passwords**. The **Password Accounts List** page appears, as shown in Figure 54 "Password Accounts List" (page 172).
3	Next to **Password Basic Parameters**, click **Edit**.

The **Password Basic Parameters** page appears, as shown in Figure 58 "Password Basic Parameters" (page 179).

Figure 58
Password Basic Parameters



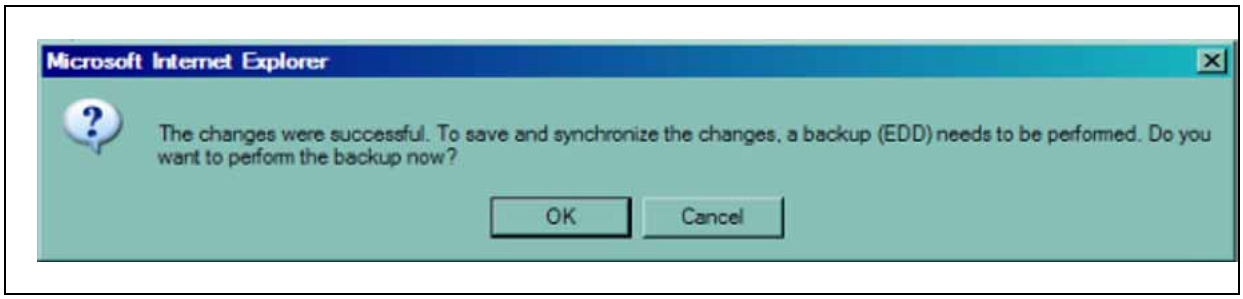
4 Edit any of the following parameters by selecting or clearing the check box, selecting from the list, or entering a value in the field:

- Force Password Change
- Failed Log in Threshold
- Failed Log In Threshold Alarm
- Port Lockout Time After Failed Log in
- Password Complexity Check
- Auto Trail for Password Usage
- Word Size of Audit Trail Buffer
- Last Log In Identification
- Inactivity Timeout

5 Either:

Click **Save** to save the changed password settings, and return to the **Password Accounts List** page. The following message appears:

Figure 59
EDD confirmation



OR

Click **Cancel** to cancel the changes, and return to the **Password Accounts List** page

6 Either:

Click **OK** to perform an EDD.

OR

Click **Cancel** to return to the **Password Accounts List** page.

—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 178).

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 181))
- switchroom security (see "Switchroom security" (page 182))
- network facilities security (see "Network facilities security" (page 182))

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 160).

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 28 "System keys that must be manually refreshed" (page 183).

Table 28
System keys that must be manually refreshed

Key	For more information see:
SSH	"Manage SSH keys using overlays" (page 189) or "SSH key management using Element Manager" (page 194)
ISSS	"ISSS configuration from the call server using overlays" (page 131) and "ISSS configuration using Element Manager" (page 142)

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 Services 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-protected. 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 21).

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.

Procedure 81

Managing secure shell access by using LD 117

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
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 29 "Job aid: shell management commands in LD 117" (page 186).

Table 29
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 29 "Job aid: shell management commands in LD 117" (page 186).

Procedure 82
Managing insecure shell access by using LD 117

Step	Action
1	Log on using an account that has SEC_ADMIN privilege.
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 30 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 187).

Procedure 83
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 30 "Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices" (page 187).

—End—

Table 30
Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices

Command	Description
disInsecureShells	Use this command to disable all insecure shells in the system. This includes Telnet and rlogin sessions.
enlInsecureShells	Use this command to enable all insecure shells in the system. This includes Telnet and rlogin sessions.
statInsecureShells	Use this command to display the status of the insecure shell access.

Enable or disable shell access using Element Manager

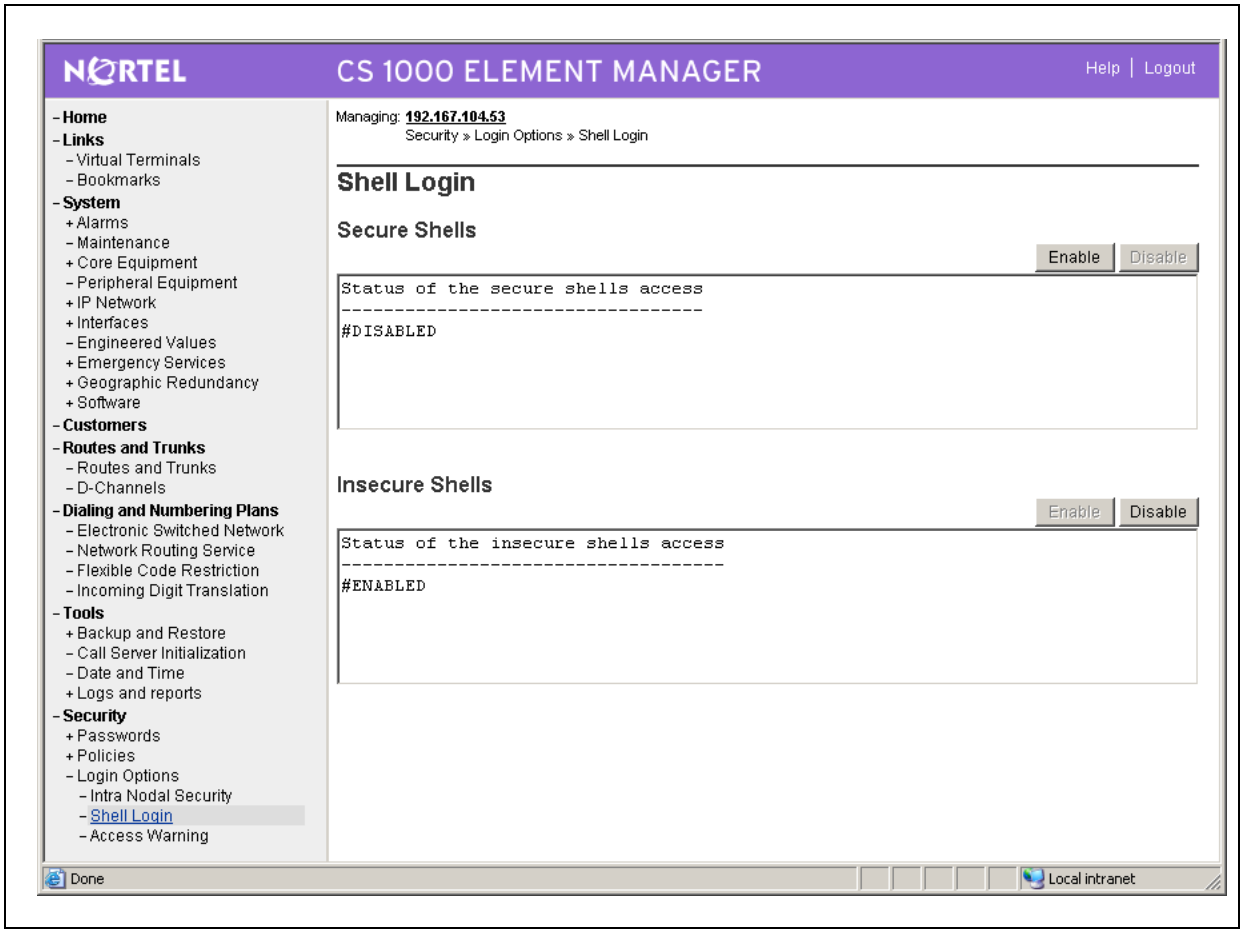
Use the following procedure to check the status of secure or insecure shells using Element Manager, or to enable or disable secure shells or insecure shells.

Procedure 84

Enabling or disabling shell access using Element Manager

Step	Action
1	Log on to Element Manager using an account that has PWD2 privilege.
2	Click **Security > Login Options > Shell Login**. The status of secure shell access appears in the Secure Shells pane, as shown in Figure 60 "Shell Login " (page 188).

Figure 60
Shell Login



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.

Procedure 85

Accessing the system remotely

Step	Action
1	Either: To log on using the same user name you used to log on to the remote terminal, enter the command **`$ ssh2 remote.example.org`**, where remote.example.org is the address of the system you are accessing. **OR** To log on using another user name, enter the command **`$ ssh2 -l username remote.example.org`**, where remote.example.org is the address of the system you are accessing.

—End—

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.

Procedure 86

Generating SSH keys by using LD 117

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.
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 31 "Job aid: arguments for SSH KEY GENERATE" (page 190).

The generated key is stored in a pending state until it is activated.

—End—

Table 31
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.

Procedure 87
Activating SSH keys by using LD 117

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.
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 32 "Job aid: arguments for SSH KEY ACTIVATE" (page 190).

—End—

Table 32
Job aid: arguments for SSH KEY ACTIVATE

Command argument	Purpose
`SSH KEY ACTIVATE`	To activate the pending key by restarting the SSH server on the call server.
`SSH KEY ACTIVATE ACTIVE`	To activate the pending key by restarting the SSH server on the active core in a two-CPU system.

SSH KEY ACTIVATE INACTIVE	To activate the pending key by restarting the SSH server on the inactive core in a two-CPU system.
SSH KEY ACTIVATE CABINET [n]	To activate the pending key by restarting the SSH server on the expansion cabinet or MG1000E. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

Use the following procedure to view SSH keys from the call server.

Procedure 88
Viewing SSH keys by using LD 117

Step	Action
1	Log on to the system.
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 33 "Job aid: arguments for SSH KEY SHOW" (page 191).

—End—

Table 33
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 81 "Managing secure shell access by using LD 117" (page 185).

Procedure 89
Clearing SSH keys by using LD 117

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.
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 34 "Job aid: arguments for SSH KEY CLEAR" (page 192).

—End—

Table 34
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 90
Generating SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.

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 91
Activating SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.
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 92
Viewing SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the system.
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. You must disable secure shells before you can clear SSH keys.

Procedure 93

Clearing SSH keys by using OAM, PDT, or IPL

Step	Action
1	Log on to the system using a user name that has SEC_ADMIN privilege.
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

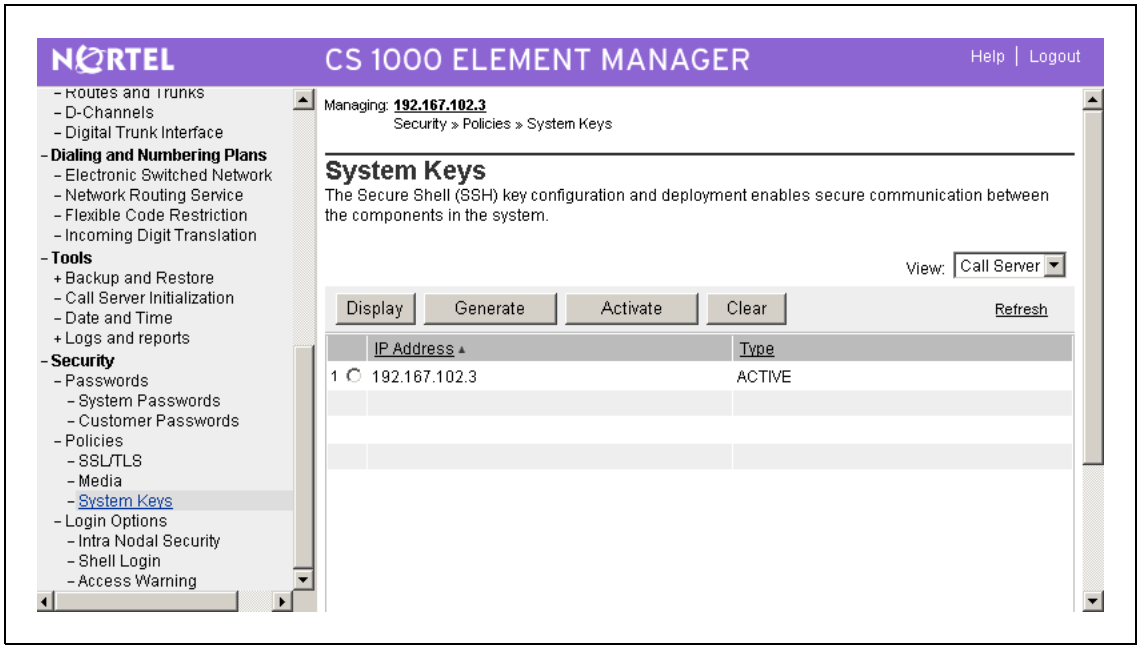
In Element Manager, you can use the System Keys page to display, generate, activate, or clear Secure Shell (SSH) keys for the Call Server, IP Media Gateway (IPMG), Signaling Server and Voice Gateway Media Card.

Procedure 94

Managing SSH keys by using Element Manager

Step	Action
1	Log on to Element Manager using a user name that has SEC_ADMIN privilege.
2	Click **Security > Policies > System Keys** . The **System Keys** page appears, as shown in Figure 61 "System Keys " (page 195).

Figure 61
System Keys



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.

Procedure 95

Viewing the banner by using LD 117

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
2	At the LD 117 => prompt, enter **BANNER SHOW** . The current banner text appears.

—End—

Procedure 96

Loading a new banner by using LD 117

Step	Action
1	Using an ASCII text editor, edit the banner.txt file to contain the new message.

2 Save the updated banner.txt files using the file name `/u/pub/banner.txt`.

3 Log on to the system using an account that has SEC_ADMIN privilege.

4 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 200).

Use the following procedure to restore the default text to the logon banner. Table 12 "Default text of the customizable logon banner" (page 44) shows the default text.

Procedure 97

Restoring the default banner by using LD 117

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 200).

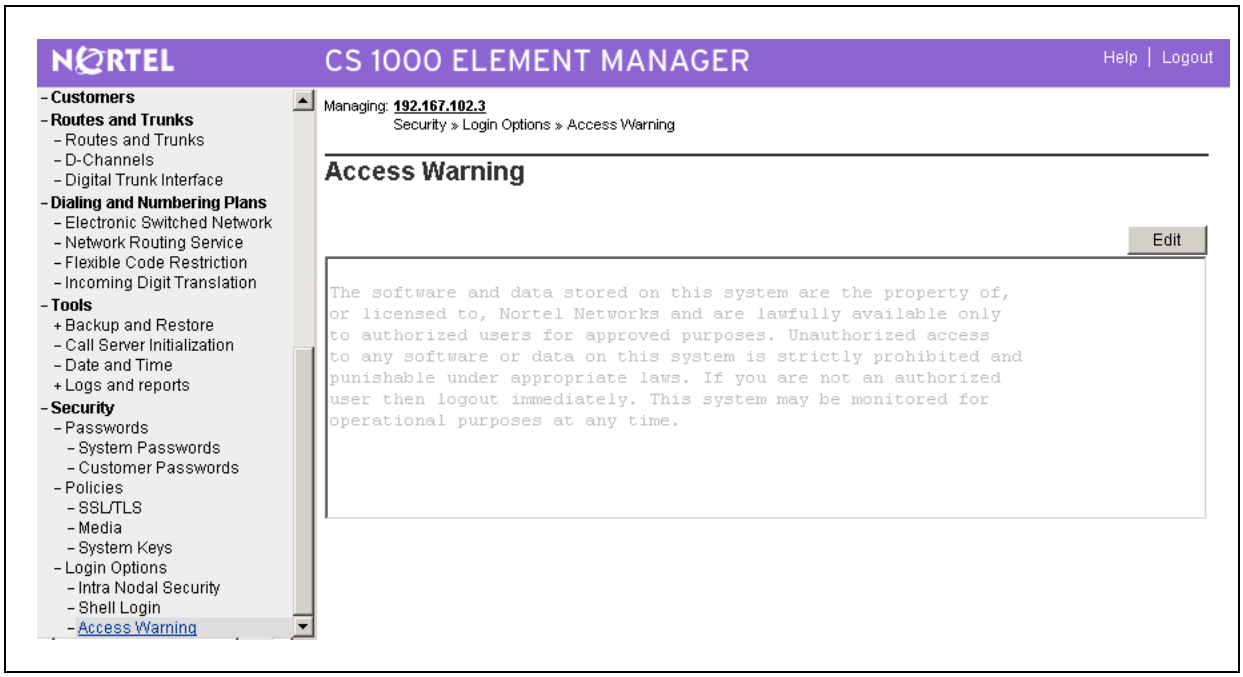
Manage the custom logon banner using Element Manager

Use the procedures in this section to view or change the logon banner, or restore the default logon banner using Element Manager.

Procedure 98
Viewing or editing the custom banner text by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Login Options > Access Warning** . The **Access Warning** page appears, as shown in Figure 62 "Access Warning" (page 198).

Figure 62
Access Warning



3	Click **Edit**. The Edit Login Banner page appears. You can view the existing banner text on this page.
4	Either: Edit the banner text. **OR** Click **Cancel** to exit the **Access Warning** page.
5	Either: Click **Save** to save and distribute the new banner file. **OR**

Click **Cancel** to cancel the changes.

6 If you choose Save in Step 5, a confirmation dialog box appears. Either:

Click **OK** to save and distribute the banner file.

OR

Click **Cancel** to cancel the changes.

—End—

Use the following procedure to restore the default text to the logon banner. Table 12 "Default text of the customizable logon banner" (page 44) shows the default text.

Procedure 99

Restoring the default banner by using Element Manager

Step	Action
1	Log on to Element Manager using an account that has SEC_ADMIN privilege.
2	Click **Security > Login Options > Access Warning** . The **Access Warning** page appears, as shown in Figure 62 "Access Warning" (page 198).
3	Click **Reset**. The Edit Login Banner page appears.
4	Edit the banner text.
5	Either: Click **Save** to save and distribute the new banner file. **OR** Click **Cancel** to cancel the changes.
6	If you choose Save in Step 5, a confirmation dialog box appears. Either: Click **OK** to save and distribute the banner file. **OR** Click **Cancel** to cancel the changes.

—End—

Force an EDD using overlays

Many configuration changes on the system do not take effect until an Electronic 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.

Procedure 100
Forcing an EDD by using LD 43

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.
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 acct_002.db and banner.txt, are also distributed to attached devices if the system is rebooted.

Security debugging

This chapter provides information and procedures to help you perform debugging of security features. The chapter is divided into the following sections:

Debug tools are not required during normal operation of the Communication Server 1000 (CS 1000) system.

Media Security debug tools

Media Security debug tools are provided to debug system problems, such as voice quality problems or echo.

The Media Security feature establishes cryptographic contexts for securing media packets between endpoints. The system protects the media stream by encrypting media packet payloads and authenticating both payloads and the headers. To avoid compromising this security, debug tools for Media Security are only available in a separate debug mode, and the debug mode can be enabled only by a user that has SEC_ADMIN privilege. When enabling debug mode, you can enable it only on specified terminals, which leaves the rest of the terminals in the system secure. Further, the debug mode is turned off after a configurable period of time.

Enable or disable Media Security debug mode

The Media Security debug mode is disabled by default. Use the following procedure to enable Media Security using commands in LD 80, and to control how long it remains enabled.

Procedure 101

Enabling Media Security debug mode by using LD 80

Step	Action
1	Log on to the system using an account that has SEC_ADMIN privilege.

2 At the LD 80 prompt, enter **EMSD <user-name> <time-out>** to grant the specified user access to the Media Security debug mode for terminals, nodes, and bandwidth management zones.

For more information about the arguments for this command, see Table 35 "Job aid: arguments for the EMSD command" (page 202).

The Media Security debug key appears in the form of a 64 bit hex value. The key is unique to the current debug session, and is not stored by the system. You must manually record the key if you want to access debug files after the debug session has ended.

—End—

Table 35
Job aid: arguments for the EMSD command

Command Argument	Description
<user-name>	Enter the PDT2 user name to which you want to grant debug access. Only one account can have this permission at any point in time.
<time-out>	Enter the period of time after which the Media Security debug mode is disabled on all terminals, and the system returns to normal operation. Configurable in hours and minutes: <time-out> = <XXX XX> = hours minutes. The default time is 003 00 (3 hours). Configurable in 1 minute intervals to a maximum of 240 00 (10 days).
Example: **EMSD norteluser 024 00**. Use this command to enable Media Security debug mode for the user name norteluser, for a period of 24 hours.	

Use the following procedure to manually disable access to the Media Security debug mode.

Procedure 102
Disabling Media Security debug mode by using LD 80

Step	Action
1	Log on to the system using an account that has PDT2 privilege.
2	At the LD 80 prompt, enter **CMSD**.

—End—

View information about Media Security debug

Use the following procedure to view information about the Media Security debug mode, including:

- the name of the user account currently assigned Media Security debug privilege
- the time and date when the mode was last enabled or disabled
- the current status (enabled or disabled)
- the time remaining before Media Security debug mode is automatically disabled

Procedure 103

Viewing information about Media Security debug mode by using LD 80

Step	Action
1	Log on to the system using an account that has PDT2 privilege.
2	At the LD 80 prompt, enter **PMSD**.

—End—

Use the following procedure to view information about the Media Security debug mode key used for file encryption. The key is printed in hex format (a 64 bit key is represented in 16 hex characters). Old keys are overwritten and destroyed, so the key that this procedure displays is the one used in the current Media Security debug mode session.

Procedure 104

Viewing information about the current Media Security debug mode key by using LD 80

Step	Action
1	Log on to the system using an account that has PDT2 privilege.
2	At the LD 80 prompt, enter **KMSD**. The key appears. If Media Security debug mode is not enabled, an error appears.

—End—

Use Media Security Debug

Media Security debug mode offers two modes of operation, as described in Table 36 "Media Security debug modes of operation" (page 204).

Table 36
Media Security debug modes of operation

Debug mode	Description
Media Security override in debug mode for specific terminals	Use this mode to disable media encryption for specific selected terminals, nodes and bandwidth management zone. Enable this option to cause the selected endpoints to transmit unencrypted media. All other terminals operate normally.
Media Security enabled in debug mode for specific terminals	Use this mode to decrypt the traffic between specified terminals. Enable this option to cause the media stream for the selected terminals, nodes, and bandwidth management zone to be encrypted using dynamically generated keys. The keys are stored in a file, and you can use them to decrypt the encrypted media stream.

Use the following four commands to enable or disable Media Security debug mode on specific terminals:

- secDebugOverrideEnable
- secDebugOverrideDisable
- secDebugEnable
- secDebugDisable

To get help for any of these commands, enter them without arguments at the PDT prompt. For more information about how to enable or disable Media Security debug mode, see "Media Security override in Debug mode for specific terminals" (page 204).

Media Security override in Debug mode for specific terminals

Use the following procedures to enable or disable Media Security override in Debug mode for specific terminals using the command line interface (CLI). Enabling this feature temporarily turns off encryption on specified terminals; a timer controls the amount of time before Media Security resumes normal function. The specified terminals continue to operate normally.

Procedure 105
Enabling Media Security override in Debug mode for specific terminals by using CLI

Step	Action
1	Log on to the system using an account that has PDT2 privilege.

2 At the PDT2 prompt, enter either:

```
secDebugOverrideEnable tn <TN_range_start>
<TN_range_end> [<time-out>]
```

OR

```
secDebugOverrideEnable dn <DN_range_start>
<DN_range_end> [<time-out>]
```

OR

```
secDebugOverrideEnable node <node_range_start>
<node_range_end>
```

OR

```
secDebugOverrideEnable zone <zone_range_start>
<zone_range_end> [<time-out>]
```

—End—

Procedure 106

Disabling Media Security override in Debug Mode for specific terminals by using CLI

Step	Action

1 Log on to the system using an account that has PDT2 privilege.

2 At the PDT2 prompt, enter either:

```
secDebugOverrideDisable tn <TN_range_start>
<TN_range_end>
```

OR

```
secDebugOverrideDisable dn <DN_range_start>
<DN_range_end>
```

OR

```
secDebugOverrideDisable node <node_range_start>
<node_range_end>
```

OR

```
secDebugOverrideDisable zone <zone_range_start>
<zone_range_end>
```

—End—

Media Security enabled in Debug Mode for specific terminals

Use the information in this section to debug Media Security by decrypting traffic packets between specified terminals, while continuing to use encryption for the media traffic. This approach limits access to the media stream to users who possess the dynamically generated key. Terminals placed in this mode continue to operate normally.

A timer controls the amount of time before Media Security resumes normal function.

Use the following procedures to enable or disable Media Security enabled in Debug Mode for specific terminals.

Procedure 107

Enabling Media Security enabled in Debug Mode for specific terminals by using CLI

Step	Action
1	Log on to the system using an account that has PDT2 privilege.

2	At the PDT2 prompt, enter either:
	`secDebugEnable tn <TN_range_start> <TN_range_end> [mode] [rekeying_time]`
	OR
	`secDebugEnable dn <DN_range_start> <DN_range_end> [mode] [rekeying_time]`
	OR
	`secDebugEnable node <node_range_start> <node_range_end> [mode] [rekeying_time]`
	OR
	`secDebugEnable zone <zone_range_start> <zone_range_end> [mode] [rekeying_time]`
	For more information about the arguments for this command, see Table 37 "Job aid: arguments for Media Security debug mode on specific terminals" (page 207).

—End—

Procedure 108
Disabling Media Security enabled in Debug Mode for specific terminals by using CLI

Step	Action
1	Log on to the system using an account that has PDT2 privilege.

2	At the PDT2 prompt, enter either:
	`secDebugDisable tn <TN_range_start> <TN_range_end>`
	OR
	`secDebugDisable dn <DN_range_start> <DN_range_end>`
	OR
	`secDebugDisable node <node_range_start> <node_range_end>`
	OR
	`secDebugDisable zone <zone_range_start> <zone_range_end>`
	For more information about the arguments for this command, see Table 37 "Job aid: arguments for Media Security debug mode on specific terminals" (page 207).

—End—

Table 37
Job aid: arguments for Media Security debug mode on specific terminals

Command Argument	Description
[mode]	
[rekeying_time]	
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
tn	
dn	
node	
zone	

<TN_range_start> <TN_range_end>	
<DN_range_start> <DN_range_end>	
<node_range_start > <node_range_end>	
<zone_range_start> <zone_range_end>	

View information about Media Security Debug

Use the following procedure to view the following information:

- all terminals, nodes and zones that have Media Security debug mode enabled
- the time remaining before Media Security debug mode is automatically disabled on each terminal, node, and zone
- the hard drive, file location, and file size for the msdmXXX.log

Procedure 109

Viewing information about Media Security debug by using CLI

Step	Action
1	Log on to the system using an account that has PDT2 privilege.
2	At the PDT2 prompt, enter **`secDebugPrintAll`**.

—End—

IPsec debug tools

Use the information in this section to debug IP Security (IPsec).

Use the following procedure to decommission IPsec locally using the OAM, PDT, or IPL prompt.

Procedure 110

Decommissioning IPsec locally by using CLI

Step	Action
1	Log on using an account that has PWD2 and PDT2 privileges.
2	At the OAM, PDT, or IPL prompt, 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 111
Viewing IPsec profile information by using CLI

Step	Action
1	At the OAM, PDT, or IPL prompt, enter **isecProfileShow**. All IPsec profile information appears.

—End—

Use the following procedure to generate salt values and hashed system preshared key (PSK), and to display them, along with system security status and system security level.

Procedure 112
Confirming IPsec system settings on the active call server by using CLI or LD 117

Step	Action
1	Either: At the LD 117 prompt, enter **CONFIRM ISEC**. **OR** At the OAM, PDT, or IPL prompt, enter **isecConfirm**. The salt value, hashed PSK, system security status and system level appear.

—End—

Use the following procedure to generate salt values and hashed system PSK.

Procedure 113

Confirming IPsec system settings on devices other than the active call server by using CLI or LD 117

Step	Action
1	Either: At the LD 117 prompt, enter **CONFIRM ISEC <salt value>**. **OR** At the OAM, PDT, or IPL prompt, enter **isecConfirm <salt value>**. The hashed PSK, system security status, and system level appear.

—End—

Use the following procedure to view connection information for IPsec.

Procedure 114

Viewing IPsec connection information by using CLI

Step	Action
1	At the OAM, PDT, or IPL prompt, enter **isecIkeShowSAll**. 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 115
Viewing IPsec network interface information by using CLI

Step	Action
1	At the OAM, PDT, or IPL prompt, 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.

Procedure 116
Viewing IPsec configuration by using LD 117

Step	Action
1	At the LD 117 prompt, enter either: **`prt ISEC {all|excep|target|syc}`** **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.

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 now 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 38 "LD 2: Using invs 16 to access OMs" (page 214).

Table 38
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 39 "Media Security OMs" (page 214)

Table 39
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 40 "SIP TLS OMs" (page 215) shows the operational measurements (OMs) relating to Transport Layer Security for Session Initiation Protocol (SIP TLS) that are logged by the SIP Gateway.

Table 40
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 41 "SIP TLS alarms" (page 216) shows the alarms relating to TLS that appear on the Signaling Server console as ERROR system logs (syslogs).

Table 41
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
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 42 "Encryption technologies used in CS 1000" (page 218) lists encryption technologies used in CS 1000 Release 5.0.

Table 42
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. These certificates are either self-signed by the originator of a message, or are signed by a trusted third party certificate authority (CA). Some systems refer to certificates as X.509 certificates; this refers to a standard method of formatting the 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

Electronic 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 for securing internet protocol (IP) communications by encrypting and authenticating all 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 protocols operate at the network layer, Layer 3 of the OSI model. Other Internet security protocols, such as SSL and TLS, operate from the transport layer up (OSI Layers 4 to 7). This makes IPsec more flexible, because IPsec can protect both TCP and UDP-based protocols, but increases its complexity and processing overhead, because it cannot rely on TCP (Layer 4 of the OSI model) to manage reliability and fragmentation.

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

NRSM

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 proposed standard 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 servers and other SIP endpoints. 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

The Secure Real-time Transport Protocol (or SRTP) defines a profile of Real-time Transport Protocol (RTP). SRTP provides encryption, message authentication and integrity, and replay protection to RTP data in both unicast and multicast applications. Because RTP is closely related to RTCP (RTP control protocol), which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (SRTCP). SRTCP provides the same security-related features to RTCP, as the ones provided by SRTP 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 on the Internet for applications such as e-mail, Internet fax, and other data transfers that require security. TLS provides endpoint authentication and communications privacy over the Internet by using cryptography. In many applications, only the server is authenticated, and the client is unauthenticated. Mutual authentication 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

K

L

M

N

P

Nortel Communication Server 1000

Security Management Fundamentals

Publication: NN43001-604
Document status: Standard
Document version: 01.05
Document date: 30 May 2007

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

Sourced in Canada