Avaya Communication Server 1000 Security Management Fundamentals

Release 7.6
NN43001-604
Issue 06.06
September 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

The following sections detail what is new in *Avaya Security Management Fundamentals, NN43001-604* for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.6.

Features

There are no updates to the feature descriptions in this document.

Other changes

There are no other changes.

Revision history

September 2015	Standard 06.06. This document is up-issued to include descriptions for the Client Authentication and Periodic Re-keying fields.
December 2014	Standard 06.05. This document is up-issued to include updates to exclude content related to DTLS client authentication and periodic rekeying.
September 2014	Standard 06.04. This document is up-issued to include updated information about environments that support media security/sRTP.
June 2014	Standard 06.03. This document is up-issued to include content about cryptographic algorithm SHA2 (SHA–256 with RSA) with increasing default key length from 1024 to 2048.
November 2013	Standard 06.02. This document is up-issued to support Mozilla Firefox 19.0 and later.
March 2013	Standard 06.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.6.

Table continues…

March 2012	Standard 05.07. This document is up-issued for changes in the section Third-party CAs and chains of trust on page 26.
February 2012	Standard 05.06. This document is up-issued to include updates to the overlay command descriptions for enabling or disabling SFTP.
June 2011	Standard 05.05. This document is up-issued to include updates to security domain content.
April 2011	Standard 05.04. This document is up-issued to include prompt and response tables for overlay procedures and to include information about joining devices to the UCM security domain.
March 2011	Standard 05.03. This document was up-issued to support Avaya Communication Server 1000 Release 7.5. Addition made to the “ISSS Geographic Redundancy” section.
November 2010	Standard 05.01 and 05.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 04.03. This document is up-issued to support Avaya Communication Server 1000 Release 7.0. A note is added for the command isetSecUpdate.
June 2010	Standard 04.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.0. The section about IPsec configuration is updated.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
June 2009	Standard 03.04. This document is up-issued to support Communication Server 1000 Release 6.0. The section on ISSS configuration has been updated.
June 2009	Standard 03.03. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.02. This document is up-issued to support Communication Server 1000 Release 6.0.
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.
April 2008	Standard 02.08. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5, and to add support for UNIStim 3.0.
April 2008	Standard 02.07. This document is up-issued to support Communication Server 1000 (CS 1000) Release 5.5, and to add information about Media Security and SIP Phones.
March 2008	Standard 02.06. This document is up-issued to support CS 1000 Release 5.5, and to add information about Mobile Extensions.
January 2008	Standard 02.05. This document is up-issued to support CS 1000 Release 5.5.
December 2007	Standard 02.01 This document is up-issued to support CS 1000 Release 5.5.
October 2007	Standard 01.46. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related to password reset procedures.
October 2007	Standard 01.42 This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related to Intrasystem Signaling Security Solution (ISSS) configuration.

Table continues…

September 2007	Standard 01.34 This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content related primarily to ISSS configuration.
June 2007	Standard 01.13. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about SIP TLS and ISSS configuration.
May 2007	Standard 01.06. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about SIP TLS configuration, and corrections to statements about password conversion.
May 2007	Standard 01.03. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to information about Media Security configuration.
May 2007	Standard 01.02. This document is up-issued to support CS 1000 Release 5.0, and to reflect changes in technical content, including changes to NKEY configuration ranges.
May 2007	Standard 01.01. This document is issued to support CS 1000 Release 5.0 This document contains information about security features that are new in CS 1000 Release 5.0, and about changes to existing security features. This document also contains information previously contained in the following legacy document, now retired: *System Security Management, 553-3001-302*.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: 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 Avaya Communication Server 1000 (Avaya CS 1000) system using UCM Common Services, including:

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

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

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

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

Navigation

This document includes the following chapters:

Other security information

This technical publication provides information about many of the features you can use to provide security for your Avaya Communication Server 1000 system. Some security features are described in other technical publications. For more information, see Table 1: Other technical publications that contain security information on page 17.

Table 1: Other technical publications that contain security information

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

About this document

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

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

Subject

This technical documentation contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 software and UCM Common Services. For more information about legacy products and releases, click the **Documentation** link under **Support** on the Avaya home page: http://www.avaya.com.

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

Applicable systems

This document applies to the following systems:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 software and configured to include a Signaling Server, they become CS 1000 systems.Table 2: Meridian 1 systems to CS 1000 systems on page 18 lists each Meridian 1 system that supports an upgrade path to a CS 1000 system.

Table 2: Meridian 1 systems to CS 1000 systems

This Meridian 1 system...	Maps to this CS 1000 system
Meridian 1 PBX 11C Chassis	CS 1000E
Meridian 1 PBX 11C Cabinet	CS 1000E
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81C	CS 1000M Multi Group

Intended audience

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

Terminology conventions

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

- Communication Server 1000M (CS 1000M)

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

In this document, the following Chassis or Cabinets are referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Chassis Expander (NTDK92)
- Option 11C Cabinet (NTAK11)
- MG 1000E Chassis (NTDU14) and Expansion Chassis (NTDU15)
- IPE module (NT8D37) with MG XPEC card (NTDW20)
- Media Gateway 1010 (MG 1010) (NTC310)

In this document, the following hardware is referred to as Gateway Controller:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)

In this document, the following hardware is referred to generically as Server:

- Call Server Pentium IV (CP PIV)
- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x306m server (COTS1)
  - HP DL320 G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

Co-res CS and SS is not supported on COTS1 servers. You can deploy a COTS1 server as a stand-alone Signaling Server.

The following table shows CS 1000 supported roles for hardware platforms.

Table 3: Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no

Table continues…

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS1	no	yes	no	no
COTS2	no	yes	yes	no

Note:

The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying slot 0 in a Media Gateway.

In this document, the following terminology applies:

- On systems where System Manager is available, the term UCM in the documentation refers to UCM in System Manager; on systems where System Manager is not available, the term UCM in the documentation remains unchanged.
- On systems where Session Manager is available, the term NRS in the documentation refers to Session Manager; on systems where Session Manager is not available, the term NRS in the documentation remains unchanged.

Chapter 4: Fundamentals of system security management

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

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

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

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

Important:

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

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

- Most ELAN subnet communication is protected by ISSS/IPsec. The following components connect through their ELAN interfaces to the ELAN subnet, where communication is protected by ISSS:
  - Element Manager ELAN interface
  - CP Side 0 and CP Side 1 of the CS 1000 logical Call Server (LCS) with the high availability option
  - Co-resident Call Server and Signaling Server

  - Signaling Servers associated with a specific Call Server
  - Voice Gateway Media Cards (VGMC) and Gateway Controllers in collocated IP Media Gateways (IPMG)

  All systems include an ELAN subnet to which the CS1000 Call Server ELAN interface and its collocated system elements connect. The Gateway Controller and its DSP resources exchange control information using their ELAN interface.

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

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

System security overview

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

- Platform security
  - Linux security hardening
  - Signaling encryption, which prevents theft of service, spoofing, and Denial of Service (DoS)
  - System hardware and software is designed to provide hardening and protection against Denial of Service (DoS) attacks
- Security management
  - Central authentication
  - Strong password management

  - Web-based management that is secured by Secure Sockets Layer (SSL)
  - CLI-based management that is secured by SSH
  - Security logs and alarms provide accountability and notification
  - Secure billing records protects confidentiality, theft of service
- Voice Media Security
  - Signaling and Media encryption ensures voice confidentiality and privacy
  - Client Authentication controls access to services

General signaling security overview

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

Key management concepts

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

Key generation

The strength of an encryption system depends on two factors:

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

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

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

Key exchange

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

- Distributed to the individual endpoints by a central server. This method requires that the distribution itself be secured to reduce the risk of corruption or interception of the keys. Media Security keys and ISSS pre-shared keys are shared using this method.
- Pre-shared between endpoints in the system. You can manually configure pre-shared keys used by some features. Pre-shared keys for manually added ISSS targets are shared using this method.

- Exchanged using a certificate with public-private key pairs. The certificate of the server is sent in the initial handshake. The public key of the server is used to encrypt a random session key, which is then transmitted. The server then uses the unique private key to decrypt the generated session key and obtain a unique shared session key, which is used by both sides during the term of the session.

  Element Manager, Unified Communications Management, DTLS, and SIP TLS keys are exchanged using this method. The certificate contains a digital signature that verifies the identity of the owner of the public key in the certificate. Certificates are either self-signed, or signed by a CA:

  - Some features can use certificates that are self-signed, but self-signed certificates do not provide authentication and are not scalable.
  - Certificates issued by a local private CA or a public CA use Public Key Infrastructure (PKI). Third-party signed certificates can usually provide authentication and are scalable.
- For more information about public-key certificates, see Public-key certificate concepts on page 24.

Public-key certificate concepts

Overview

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

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

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

The certificate chain is a series of certificates provided by the CA issuing the certificates to the endpoints. The certificate chain begins with the peer certificate and completes with the root

certificate of the hierarchy. Each certificate is signed with the private key of the issuer, which can be verified with the public key of the next certificate in the chain. To be successfully imported into the Signaling server using Unified Communications Management, the certificates must be compiled into a single PEM file.

Certificate management

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

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

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

Certificate types

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

- Self-signed certificates. Self-signed certificates are not issued by a CA. This type of certificate does not provide secure authentication and is vulnerable to third-party intercepts. Avaya recommends that you avoid using self-signed certificates whenever possible.
- Certificates signed by the private CA hosted on UCM primary security server. During the installation of the Unified Communications Management primary security server, a private CA is created. You can use the private CA to issue certificates to remote devices in the same security domain.

  When a certificate is issued from Unified Communications Management primary security server and distributed to a remote device, the root certificate of the private CA is automatically added to the trusted certificate list on that device. As a result, devices that use certificates issued by the same private CA always trust each other.

  Note:

  Quantum Certificate authority provides a private CA for the Quantum framework. With the Quantum Certificate authority, you can use functionality such as signing Certificate Signing Requests (CSRs) to issue certificates, revoking issued certificates, and providing lists of

issued and revoked certificates. From Release 7.6 onwards, certificate digital signatures are done using SHA-256 (with RSA). CSR generators also use SHA-256 (with RSA) signature algorithm.

- Certificates signed by a public CA. A public CA can be an existing internal CA from within your organization or an outside commercial CA (such as Verisign or Thawte). You can use the Unified Communications Management X.509 certificate management console to generate a Certificate Signing Request (CSR) from a target device and transfer it to a public CA for a certificate response containing an X.509 certificate.

  You can then use the Unified Communications Management certificate management console to process the certificate response returned from a public CA and distribute the X.509 certificate to the target device.

Trusted certificates list

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

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

Third-party CAs and chains of trust

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

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

Table 4: Examples of certificates in a chain on page 27 shows examples of the certificates included in a chain.

Table 4: Examples of certificates in a chain

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

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

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

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

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

Note:

The public CA certificate must be added to all servers in the domain.

A CA certificate is a public CA certificate if the basicConstraints CA value is set to TRUE; for example:

```
X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
```

Certificate management and SSL/TLS configuration

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

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

For certificate and CA management procedures, see Certificate Management on page 85.

Platform security overview

This section provides an overview of platform security features.

Unified Communications Management security services

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

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

For information about Unified Communications Management authentication methods, see Authentication methods on page 253.

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

Unified Communications Management security server roles

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

Primary security server role

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

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

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

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

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

Backup security server role

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

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

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

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

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

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

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

Member security server role

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

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

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

Security Domain Manager concepts

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

proper system operability and security, all elements in a system must be members of the same UCM security domain.

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

Note:

sFTP must be enabled on the system for elements to join the security domain.

For the full list of commands for adding or removing elements from the UCM security domain, see Add or remove elements from the UCM security domain on page 227.

Linux security hardening

Linux security hardening is divided into the following two categories:

- Basic hardening
- Enhanced hardening

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

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

Basic hardening

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

Basic hardening items are turned on by default and they are not configurable. Although Basic hardening items are turned on by default, there can be instances where you can reapply Basic hardening values. For example, you can reapply Basic hardening after the installation of third-party applications to ensure that all Basic hardening items are in secure status. Use the CLI command **`harden basic`** to perform this task.

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

Enhanced hardening

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

Table 5: Enhanced hardening default values

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

Note:

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

Note:

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

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

  Note:

  If you manipulate the SSH filter, ensure the IP and subnet values are correct. Incorrect IP and subnet values will cause you to lose connectivity. If connectivity is lost, you must

reestablish your connection using the console. If you configure SSH filtration, ensure that all members of the security domain are in the filtration list.

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

  Note:

  When the **harden coredumps off** command is issued, a system restart is necessary for the command to take effect.
- Enable or disable the Linux Audit daemon. Use the CLI command **harden audit on[off]** to perform this task.

  Note:

  If audit logs are enabled, you must provide storage for audit data. The logs will take up space until auditing is turned off.
- Enable or disable Trivial File Transfer Protocol (TFTP) service. Use the CLI command **harden tftp** to perform this task.
- Enable or disable File Transfer Protocol (FTP) service. Use the CLI command **harden ftp** to perform this task.
- Enable or disable telnet service. Use the CLI command **harden telnet** to perform this task.
- Enable or disable network tools (ethereal/wireshark, tcpdump, tracepath, traceroute). Use the CLI command **harden nettools** to perform this task.

  Note:

  To use network analysis tools, the tools must be enabled by the administrator.

  Packages tcpdump, ethereal and ethereal-gnome, and commands traceroute, traceroute6, tracepath and tracepath6 are disabled in Avaya Linux base CS 1000. To enable these packages and commands use the **harden nettools on** command.
- Retrieve the status of enhanced hardening options. Use the CLI command **harden status** to perform this task.

Table 6: Linux base CLI harden commands on page 33 lists the CLI hardening commands and their description.

Table 6: Linux base CLI harden commands

Command	Description
harden audit on	Apply hardening to Audit Daemon.
harden audit off	Remove hardening from Audit Daemon.
harden audit status	Display the status of the Linux Audit Daemon.
harden banners set/file	Modify the banner text. The banner text will be replaced by the content from the file.
harden banners status	Enable or disable the pre-login banners.
harden basic	Apply basic hardening changes. Ensures that the basic hardening items are in secure status.
harden coredumps status	Enable or disable the coredump service.
harden ftp on	Apply hardening to FTP service.
harden ftp off	Remove hardening from FTP service.
harden ftp status	Display if FTP service is turned on or off.
harden help	Display help information for using the command.
harden nettools status	Enable or disable the nettools service.
harden nfs status	Display if NFS is turned on or off.
harden nfs on	Turn NFS on to manipulate NFS hardening.
harden nfs off	Turn NFS off to disable NFS.
harden nfs help	Display help information for using the command.
harden passwd_days off	Disable previously configured parameters.
harden passwd_days on	Enable previously configured parameters.
harden passwd_days set -max	Set the value of the PASS_MAX_DAYS parameter. The default value is 90.
harden passwd_days set -min	Set the value of the PASS_MIN_DAYS parameter. **Note:** This parameter must be set to a value > or = 1. The default value is 1.
harden passwd_days status	Provide the current value of the parameters from hardening storage.
harden rlogin on	Apply hardening to remote logins.
harden rlogin off	Remove hardening from remote logins.
harden rlogin status	Display if hardening for remote logins is on or off.
harden ssh_filter add -allow -subnet	Add a subnet to the allowed list. Command format is as follows: `harden ssh_filter add -allow -subnet <subnet_IP address>/<subnet_mask>`

Table continues…

Command	Description
harden ssh_filter del -allow	Delete a host IP 1 from the allowed list.
harden ssh_filter del -allow -IP	Delete a host IP from the corresponding (allow or deny) filtration list.
harden ssh_filter del -allow -subnet	Delete a subnet to the allowed list. Command format is as follows: `harden ssh_filter del -allow -subnet <subnet_IP address>/<subnet_mask>`
harden ssh_filter add -deny -IP	Add a host to the deny list.
harden ssh_filter del -deny -IP	Delete a host IP from the deny list.
harden ssh_filter del -deny <number>	Delete a host IP from the corresponding filtration list. Each host entity (per line) has logical ordinal number in XML file storage. <number> is this sequence number.
harden ssh_filter status	Display the list of the names of the hosts which are allowed to connect to Linux base by SSH.
harden status	Retrieve the status of Linux base Enhanced Hardening options.
harden telnet on	Apply hardening to telnet service.
harden telnet off	Remove hardening for telnet service.
harden telnet status	Display if telnet service is turned on or off.
harden tftp on	Apply hardening to TFTP service.
harden tftp off	Remove hardening for TFTP service.
harden tftp status	Display if TFTP service is turned on or off.

Virus protection

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

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

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

BIOS setting and password protection

To secure the server, Avaya recommends the following:

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

  Note:

  The CP PM BIOS does not support a password. You cannot add a BIOS password to a CP PM server.

- Add a boot loader password.

Removal of the Ctrl+Atl+Del keyboard shutdown command

The Ctrl+Alt+Del shutdown command is disabled.

Single-user-text-mode booting is disabled

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

Internal communications security overview

ISSS/IPsec

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

IPsec encrypts the data stream between the two endpoints of a connection. A preshared key (PSK) is used to authenticate the two endpoints, and an encryption key is negotiated by using IKE. ISSS settings (PSK and level) are specified as an ISSS policy that can be applied to individual Communication Server 1000 systems

ISSS/IPsec is managed and configured using the Unified Communications Management ISSS interface. Manual ISSS targets are associated with individual Communication Server 1000 systems rather than all systems in the Unified Communications Management (UCM) security domain. Manual ISSS targets are available as elements in UCM.

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

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

Important:

Previous versions of ISSS/IPsec are not supported in Communication Server 1000. When you upgrade a Communication Server 1000 system to Release 6.0 or greater, you must reconfigure IPsec by using the ISSS interface on the Unified Communications Management primary security server.

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

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

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

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

For procedures relating to ISSS/IPsec, see ISSS on page 66.

Secure File Transfer Protocol concepts

Secure Shell (SSH) Secure File Transfer Protocol (sFTP) is installed and enabled on Communication Server 1000 systems by default. This secure protocol replaces regular File Transfer Protocol (FTP) and other insecure data transfer protocols for several Communication Server 1000 applications. A list of applications using sFTP and FTP is shown in Applications using sFTP and FTP on page 38.

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

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

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

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

The following characteristics apply to sFTP:

- The public key of a sFTP server is always trusted by sFTP clients, so there is no requirement for verification.
- ISSS security for specific elements can be disabled using the UCM primary security server. When disabled, all communications from the specified IP address of the element are sent without IPsec to protect the messaging traffic to only the elements of the individual Communication Server 1000 system rather than all systems in the UCM security domain. Manual ISSS targets are available as elements in UCM. Manual targets with ISSS disabled must be configured without IPsec; communications between other elements is not affected.
- A user name and password is used by a sFTP server to authenticate a sFTP client (public key-based authentication is not supported for authenticating a sFTP client). For internal automated transfers, the UCM security token is used to construct the password.
- TFTP for transferring tone and cadence files is not changed
- Not all FTP applications use sFTP; some will continue using standard FTP
- Interactive users of sFTP have restricted directory access.

For commands and procedures related to the concepts described in this section, see Configure Secure File Transfer Protocol on page 257.

sFTP for Linux platforms

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

File transfer options for Linux and VxWorks platforms

Table 7: File transfer options for Linux and VxWorks platforms on page 37 shows the various file transfer options available for Linux and VxWorks platforms.

Table 7: File transfer options for Linux and VxWorks platforms

	Linux			VxWorks		
Method	**FTP**	**sFTP**	**TFTP**	**FTP**	**sFTP**	**TFTP**
Default	ON	ON	ON	ON	ON	ON

Table continues…

	Linux			VxWorks		
Options	OFF/ON[1]	ON	OFF/ON [1]	OFF/ON [2]	OFF/ON [3]	ON
[1] with Linux harden command						
[2] with Disable/Enable Transfer Insecure command						
[3] with Disable/Enable Transfer Secure command						

Note:

Avaya recommends that you do not disable secure transfers.

SSH client

The SSH client is implemented to facilitate access to an SSH server. There is no Command Line Interface (CLI) implementation of the SSH client for VxWorks platforms; however, there is access to the SSH client on Linux hosts. The joinSecDomain/REGISTER UCMSECURITY SYSTEM FORCE command, used for joining the Unified Communications Management security domain, uses the SSH client to communicate with the Unified Communications Management primary server but does not provide any shell level access.

Unsecured remote access methods are supported, such as rlogin and telnet, but you can disable them.

Applications using sFTP and FTP

Secure File Transfer Protocol (sFTP) is used for most file transfer operations, with the following exceptions where File Transfer Protocol (FTP) continues to be used:

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

Note:

There is no impact during an upgrade even if CallPilot is part of the system. CallPilot normally functions as a client, so it can continue to use an FTP client to communicate with a Call Server that supports both sFTP and FTP servers.

Port access restrictions concepts

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

Important:

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

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

Note:

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

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

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

Note:

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

For procedures related to the concepts described in this section, see Configure port access restrictions on page 260.

SNMP concepts

SNMP for Communication Server 1000

Communication Server 1000 elements support SNMP MIB access and SNMP traps are used to communicate fault information. You can configure different community strings for these purposes.

For information about SNMP for Communication Server 1000, refer to *Avaya Fault Management — SNMP, NN43001-719*.

SNMP for Avaya Aura® Media Server

Avaya Aura® Media Server can be deployed in a system to provide media services. Avaya Aura® Media Servers run on the Linux base and send SNMP traps using the Avaya Reliability MIB, as opposed to the Common Trap MIB used by other Communication Server 1000 applications.

Network management systems receiving SNMP traps from Avaya Aura® MS elements receive both Avaya Reliability MIB (Avaya Aura® MS) and Common Trap MIB (Communication Server 1000) formats. Avaya Aura® MS, when deployed on the Linux base, only sends outgoing SNMP traps. There is no support for SNMP queries relating to the Avaya Reliability MIB.

Note:

Avaya Aura® MS only supports a single trap destination, unlike Communication Server 1000 Common MIB traps that support up to eight destinations.

To send traps, you must configure the SNMP trap destination separately using the Avaya Aura® MS management interface. There is no security concern with the default community string name of `public` because it is only used for outgoing traps. The community string is visible on the same page where the trap is configured and can be altered if desired.

For information about MIBs for Avaya Aura® MS, refer to *Implementing and Administering* .

Linux Master Firewall Control

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

Media and signaling security overview

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

For example, a VPN gateway cannot prevent an illegal Real-Time Transport Control Protocol (RTCP) BYE message from closing a Real-Time Protocol (RTP) stream prematurely, nor can it stop

a malicious RTP packet from being injected into a conversation. Therefore cryptographic protection of media streams and the associated RTCP Control streams are available on the system.

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

Media Security concepts

The Media Security feature provides a means by which two endpoints capable of communication using Secure Real-Time Transport Protocol (SRTP) can engage in secure media exchanges. For procedures relating to Media Security, see Media Security on page 169.

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 on page 41.

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

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

Security icon

If you enable Media Security, supported IP Phones use SRTP to encrypt and authenticate the media stream, and the system displays a security icon on the IP Phone to indicate that the media stream is encrypted. The icon is shown in Figure 1: Security icon and text indicator on an IP Phone 2002 on page 41; 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.

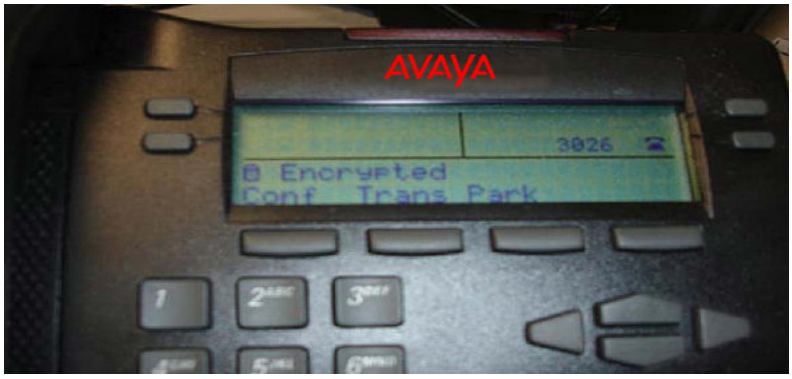


Figure 1: Security icon and text indicator on an IP Phone 2002

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/sRTP is unsupported between CS 1000 and Avaya Aura® environments.

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 on page 158.

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 should be configured as TLS never or TLS always. TLS always is also referred to as end-to-end TLS. Best effort TLS is not supported between CS 1000 and Avaya Aura® environments.

TLS protects communication between SIP endpoints by providing:

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

UNIStim signaling encryption with DTLS

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

NRS SIP Proxy

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

User and password management concepts

This section provides an overview of operations, administration, and maintenance (OAM) concepts, including information about account types, user and password management tools, and access control. For procedures relating to the concepts described in this section, see User and password management on page 196.

OAM overview

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

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

Note:

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

System accounts

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

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

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

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

Default user names and passwords are available for each of the two modes of operation, and are described in Table 9: Default user names and passwords on page 44.

Table 9: Default user names and passwords

User Name	Password				
	Call Server	**Signaling Server, Media Gateway Controller, Voice Gateway media Card**	**UCM**	**SMC 2450**	**NRS Manager**
ADMIN1 (also called PWD1 or default Level 1)	0000	Synchronized from the Call Server	na	na	na
ADMIN2 (also called PWD2 or default Level 2)	0000	Synchronized from the Call Server	na	na	na
PDT1 (also called PDT Level 1)	thorsgr8	Not applicable	na	na	na
PDT2 (also called PDT Level 2)	2tdp22ler	Synchronized from the Call Server	na	na	na
LAPW	Configured by the administrator	na	na	na	na
IP Phone Installer Password	na	na	na	na	na
admin	na	na	avaya12_Avaya	admin	admin
oper	na	na	na	oper	na

Table continues…

User Name	Password				
	Call Server	Signaling Server, Media Gateway Controller, Voice Gateway media Card	UCM	SMC 2450	NRS Manager
boot	na	na	na	ForgetMe	na
root	na	na	na	ForgetMe	na

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

The capabilities of the Level 1 account (PWD1), Level 2 account (PWD2), and PDT Level 2 account (PDT2) accounts are described in Table 10: Account level descriptions on page 45.

Table 10: Account level descriptions

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

Important:

Passwords or account changes made on the Call Server are distributed or made permanent when you perform an Equipment data dump (EDD). Similarly, when you upgrade to Communication Server 1000 Release 6.0 or greater, 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 *Avaya Telephony Services Access Control Management, NN43001-602*.

System upgrade password conversion

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

Global password settings

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

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

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

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

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

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

Role management in Unified Communications Management

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

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

There are 6 predefined roles in Unified Communication Management:

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

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

Security administration concepts

This section provides an overview of the Secure Shell (SSH) protocol, and the customizable logon banner. For procedures relating to the concepts described in this section, see Security administration on page 225.

SSH and secure remote access

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

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

Customizable logon banner

The system provides a customizable banner that appears when a user logs on to the system. The customizable banner is intended for use by customers with security policies that require network equipment to display a specific message to users when they log on. You can use this feature to display up to 20 lines of custom text, with up to 80 characters on each line. The default text of the logon banner is shown in Table 11: Default text of the customizable logon banner on page 48.

Table 11: Default text of the customizable logon banner

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

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

Chapter 5: Recommended security practices

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

- Recommendations for OAM security on page 49
- Recommendations to protect confidentiality on page 51
- Recommendations for security administration on page 52
- Security interactions on page 56
- Recommendations for upgrading to Communication Server 1000 Release 7.6 from a previous release on page 61
- Migrate existing CS 1000 Release 5.x and greater user accounts to CS 1000 Release 7.6 on page 63

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

Recommendations for OAM security

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

- password management (see User and password management on page 196)
- History File review (see History File configuration using overlays on page 214)
- Telephony Services Access Control management (see *Avaya Telephony Services Access Control Management, NN43001-602*)

Recommended password management practices

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

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

Upgrading user names from an earlier release

User names are required for all log on sessions. If you upgrade from Communication Server 1000 Release 3.0, default user names are created for any users that did not have one in the past. The names that are created for these users are shown in Table 12: User names created when accounts without user names are converted from CS 1000 Release 3.0 on page 50.

Caution:

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

Table 12: 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

Table continues…

Account	User name
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. Avaya therefore recommends that you make note of the order in which the users are listed before commencing an upgrade.

Recommendations to protect confidentiality

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

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

ISSS/IPsec recommendations

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

Preshared keys, SSH keys, and Secure FTP Token recommendations

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

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

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

TLS security for SIP trunks recommendations

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

Media Security recommendations

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

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

Recommendations for security administration

Secure Shell (SSH) provides several authentication methods; Avaya 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.

Avaya recommends that you use SSH whenever possible, and disable insecure shells (rlogin, and telnet) on the Communication Server 1000 system, except as needed. Both Secure Shell and insecure shells are enabled by default. Table 13: Examples of cases where insecure shells are required on page 52 lists some instances where insecure shells are required.

Table 13: Examples of cases where insecure shells are required

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

Table continues…

Feature or device	Insecure shell required
MRV IR-8020	If your system includes an MRV IR-8020, you must enable insecure shells because that device requires rlogin.

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

Note:

For SSH/telnet/rlogin/web access, the address must be entered in IPv4 format. IPv6 is not supported.

Certificates

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

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

SIP TLS certificates

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

Third-party certificates

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

Security code for Mobile Extensions

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

Single sign-on cookie domain

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

Upgrade from an earlier release

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

- Unified Communications Management is the central framework for security configuration, authentication, and administration.
- Existing IPsec configurations must be reconfigured using the UCM ISSS configuration interface.
- When you upgrade a SIP Gateway system from Communication Server 1000 Release 4.5 or greater to Release 6.0 or greater and plan to use a certificate signed by a public CA, Avaya recommends that you obtain the certificate before your upgrade. If you upgrade your SIP Gateway before obtaining the certificate, you will not have a certificate for immediate use after upgrading because it takes time to obtain the certificate. To obtain a certificate signed by a public CA, see Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading on page 129, and Processing a pending certificate response for SIP TLS when upgrading on page 133.
- Secure File Transport Protocol (sFTP) is enabled by default.
- To enable DTLS encryption for UNIStim signals, the Communication Server 1000 system must be upgraded to Release 6.0 or greater and the IP Phones must be DTLS-capable and have the latest firmware. Also, the system must be configured for at least Best Effort security level.

Certificate management

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

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

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

Certificate management across multiple UCM security domains

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

If you must place NRS in multiple top-level enterprise domains, Avaya recommends placing them in as few domains as possible. For more information, see Figure 15: SIP TLS with multiple security domains on page 159.

Recommendations to protect UNIStim IP Phones

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

UNIStim with DTLS recommendations

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

Prevent GARP spoof attacks

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

Note:

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

Enable layer 2 authentication for IP Phones

Avaya recommends that you enable the 802.1x layer 2 device authentication feature. 802.1x authentication protects against unauthorized access by authenticating each IP Phone that is connected to the system. Supported 802.1x types are listed in Table 14: Supported 802.1x types on page 56. For more information about configuring 802.1x authentication, see *Avaya IP Phones Fundamentals, NN43001-368*.

Table 14: Supported 802.1x types

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

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

Sign files

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

Security interactions

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

Co-resident Call Server and Signaling Server

The Co-resident Call Server and Signaling Server (Co-res CS and SS) which is capable of running the Call Server software, Signaling Server software, and System Management software on the same hardware platform operating under the RedHat Linux Operating System.

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

Note:

The Co-res CS and SS does not support an HA configuration (dual core with Active/Inactive role). For systems that require HA configuration, the VxWorks-based Call Server software must be deployed.

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

For information about Co-resident Call and Signaling Server, see *Avaya Co-resident Call Server and Signaling Server Fundamentals, NN43001-509*.

ISSS and Element Manager on VxWorks signaling server

If you configure ISSS to Full Security, you must enable Secure Socket Layer/Transport Layer Security SSL/TLS for Element Manager, or Element Manager cannot operate on VxWorks signaling server. For an overview of the interaction of ISSS with Element Manager, see Table 15: Interactions between ISSS and Element Manager web server on Signalling Server on page 57.

Table 15: Interactions between ISSS and Element Manager web server on Signalling Server

ISSS configuration option	Access Element Manager through ELAN	Access Element Manager through TLAN
Full Security	Only using HTTPS[1]	[2]Using HTTPS or HTTP
Functional Security, Optimized Security, No Security	Using either HTTP or HTTPS	[2]Using HTTPS or HTTP
[1]Note: The certificate for SSL must be installed on the signaling server"; for more information about certificate management see Certificate creation and management on page 92 [2]HTTP and HTTPS traffic on the TLAN is blocked if the Management Access in ELAN only flag is set on the Signalling Server.		

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

ISSS and Element Manager on UCM

If you are using Element Manager on UCM to manage Communication Server 1000 systems, Avaya recommends that you enable ISSS to protect confidentiality of communication between Element

Manager and the Communication Server 1000 systems. ISSS is required to protect communication between Element Manager on UCM and the Communication Server 1000 systems because Xmsg protocol is used by Element Manager on UCM to communicate with Communication Server 1000 systems, and Xmsg provides neither encryption nor authentication. You must add the UCM IP addresses as external IPsec targets on the Communication Server 1000 system Call Server, and configure ISSS/IPsec for the Communication Server 1000 system on UCM; for more information see IPsec configuration on page 71.

UCM supports a unique ISSS/IPsec preshared key (PSK) for each Communication Server 1000 system managed by UCM. In the list of elements managed by UCM, you must enter the IPsec PSK for each managed Communication Server 1000 system, and it must be the same IPsec PSK that you use to configure ISSS on the Communication Server 1000 system Call Server. Avaya recommends that you change the IPsec PSK manually every few months. For more information about secret keys that you must refresh manually, see Refresh system keys on page 255.

ISSS and Geographic Redundancy

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

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

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

For more information about the interaction of ISSS with FTP, see the following table.

Table 16: ISSS interaction with FTP

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

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

ISSS and AML

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

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

ISSS and Port Access Restrictions and Linux firewall

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

ISSS and other protocols

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

For information about adding an IPsec target manually, see Manual IPsec targets on page 76.

Media Security and call forwarding

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

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

Media Security and SIP phones

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

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

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

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

CallPilot traffic is not protected by Media Security on systems without MGC daughterboards or 32-channel Secure Media cards (MC32S). On these systems, IP Phones that are configured to use a Media Security Class of Service of Always cannot access CallPilot. For more information about the interaction of Media Security Class of Service with CallPilot access, see Table 17: Interactions between Media Security and CallPilot on systems without MGC daughterboards or MC32S on page 60.

Table 17: 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, Avaya recommends that you install CallPilot in Media Gateway Controller (MGC) cabinets.

SIP TLS security policy interaction with Failsafe NRS

The SIP TLS Secure End-to-End and Secure Local policy settings prevent the operation of Failsafe NRS. If you are configuring TLS on a system where you use, or plan to use, Failsafe NRS, Avaya recommends that you use Best Effort policy for TLS. See Table 18: Consequences of SIP trunk

security on page 61 for an explanation of the consequences of SIP TLS security configuration on Failsafe NRS.

Table 18: Consequences of SIP trunk security

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

SIP TLS interaction with SMC 2450

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

UCM backup server when UCM primary is offline

The backup server is in Read Only mode. Its main function is to provide authentication and authorization for member servers. The services in the navigation tree, such as, User Services, Security and CS 1000 services are either not available or are in view only mode. The applications in the element table are accessible and function as normal.

Recommendations for upgrading to Communication Server 1000 Release 7.6 from a previous release

The following is a high-level overview of the process for upgrading a Communication Server 1000 Release 5.x system to Release 7.6, as it pertains to system security.

Note:

This procedure does not apply to Geographic Redundancy configurations.

Prerequisites

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

Important:

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

Upgrading to Avaya Communication Server 1000 Release 7.6 from a pre-Release 6.0 system

1. Install the UCM primary security server or upgrade an existing ECM server to Communication Server 1000 Release 7.6.
2. Restore the backup data to the server.
3. Upgrade the NRS primary and backup servers to Communication Server 1000 Release 7.6.
4. On the UCM primary security server, migrate (or create) the user accounts to be used for Central Authentication.
5. Complete the following steps for each pre-Release 6.0 system:
   - If active, disable ISSS on each system and its elements by using Element Manager or the device CLI.
   - Perform an Equipment Data Dump (EDD) and obtain the backup data.
   - Remove the existing Signaling Servers from service. ISP1100 Signaling Servers are not supported in Communication Server 1000 Release 6.0 and greater and must be replaced. Existing Signaling Servers can be upgraded if they meet the hardware requirements for Communication Server Release 7.0. For information on Signaling Servers, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
   - Install and configure the new Signaling Servers. You must designate one Signaling Server as the Element Manager host as multiple instances of Element Manager are not supported in Communication Server 1000 Release 6.0 or greater. These register with the UCM security domain during Linux base configuration.
   - Upgrade the Call Servers to Communication Server 1000 Release 7.6, including database restoration. These register with the UCM security domain during Linux base configuration.
   - Upgrade the firmware on VGMCs using Element Manager. Gateway Controllers automatically update to Release 7.6 firmware using FTP.

- Register the Call Server, Gateway Controllers, and VGMCs to the UCM security domain. For information about registering to the UCM security domain, see Add or remove elements from the UCM security domain on page 227
- On the Call Server, configure Port Access Restrictions as desired for the Call Server, Gateway Controllers, and VGMCs.
- Disable insecure transfers and insecure shells as desired.
- If desired, configure ISSS defaults, add any manual targets, enable ISSS for the Call Server and its elements, then synchronize and activate. (You can defer this step until the entire network is upgraded.) For information about configuring ISSS, see IPsec configuration on page 71

6. Generate a new security token, which is then synchronized automatically to all members of the UCM security domain. For information about generating security tokens, see Regenerate the Secure FTP Token on page 255
7. On each Linux member, change the passwords for local system accounts, such as oam, pdt, root, and so on, as appropriate.

Migrate existing CS 1000 Release 5.x and greater user accounts to CS 1000 Release 7.6

This section describes the planning considerations and procedures for migrating existing Communication Server 1000 Release 6.0 user accounts to a Communication Server 1000 Release 7.6 system.

Prerequisites

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

- All Communication Server 1000 Release 6.0 IP telephony systems and networked IP telephony solutions must be deployed in an existing enterpise-level UCM security domain. Communication Server 1000 Release 6.0 TDM-only systems may be optionally deployed in an existing UCM domain or without UCM.
- When planning to upgrade Communication Server 1000 pre-Release 6.0 systems and networked IP telephony solutions, the Release 7.6 UCM security domain must already be established.
- All existing Communication Server 1000 OAM and PDT user accounts must be manually created in the Release 6.0 or greater UCM primary security server before starting to upgrade any pre-Release 6.0 Communication Server 1000 systems and system elements.
- For Communication Server 1000 IP telephony solutions, some OAM and PDT user accounts must have role-based access with the appropriate permissions for a subset of all Communication Server 1000 systems in the UCM security domain.

- System-specific CS 1000 OAM/PDT roles must be manually mapped by the UCM AAA network administrator to each individual Communication Server 1000 system element.

  Note:

  Users assigned to a predefined system role gain access to all system elements associated with that role. Multiple users may require specific access and restrictions beyond the capabilities of the default user roles. In this event, you must configure custom roles for those users.

  While you can define user access to the CLI of individual system elements using an instance of Element Manager, the only way to grant CLI access to the Signaling Servers for users assigned to custom roles is on a one-by-one basis.

- All OAM/PDT user account passwords must be reset when migrating to Release 7.6 UCM security domain and Communication Server 1000 Release 7.6. Due to password reset, each OAM/PDT account user must first access the UCM primary server by entering the FQDN of the UCM primary or backup server, or the FQDN of any registered Linux/UCM base element, and changing the initial reset password.

Migrating existing Avaya CS 1000 Release 5.x and greater user accounts to Avaya CS 1000 Release 7.6

1. For each server in the system, complete the following:
   - Log on to the Call Server using a PWD2 user account with user account management permissions.
   - Using LD 17, print out all PWD2, PWD1, PDT2, PDT1, and limited access system administration accounts.
   - Capture the print out of accounts for each system in a text file.

   To facilitate the migration of a large number of accounts, you can import the text files containing the print out of user accounts for each system into a spreadsheet of your own design.
2. Determine which existing Communication Server 1000 user accounts OAM and problem determination roles are authorized to access all Communication Server 1000 systems in the enterprise-wide UCM domain.

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

   Note:

   Access to the same roles on all UCM base elements in the UCM domain includes access to Linux/UCM base manager and Linux CLI of all UCM member elements, including all NRS instances, and UCM primary and backup servers.
3. Determine which existing Communication Server 1000 user accounts OAM and problem determination roles are authorized to access only a subset of Communication Server 1000 systems in the enterprise-wide UCM domain.

   These user accounts will migrate to the UCM AAA accounts that are mapped in the UCM primary security server to specially configured roles that have access only to specified

Communication Server 1000 Element Manager instances, and to specified Communication Server 1000 system elements.

Chapter 6: ISSS

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

Caution:

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

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

ISSS overview

Intra System Signaling Security (ISSS) provides authentication and encryption for internal signaling messages within a Communication Server 1000 system. IP security for Communication Server 1000 networks is centrally managed from the Unified Communications Management primary security server using the IPsec for Intra System Signaling Security (ISSS) management interface. ISSS employs IPsec to provide security services, including confidentiality, authentication, and anti-replay to application layer protocols. This feature includes industry-standard encryption algorithms from the openSSL Crypto Library.

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

ISSS elements are classified into the following two categories:

- UCM Targets—these elements automatically belong to the Unified Communications Management security domain without the need to add them using the Unified Communications Management ISSS management interface. An example of a Unified Communications Management target is a Call Server.
- Manual targets—these elements are manually defined through UCM elements page. To enable ISSS on such elements, they have to be manually associated with one or more Communication Server 1000 systems through the ISSS management interface. An example of a manual target is Call Pilot.

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

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

Table 19: ISSS/IPsec security levels

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

Table 20: Security levels and port protection for IPsec on page 67 shows ISSS security levels and how they relate to protected ports for IPsec:

Table 20: Security levels and port protection for IPsec

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

Table continues…

ISSS Level	IPsec protected ports	
	• 67 (UDP) • 68 (UDP) • 443 (TCP) • 636 (TCP) • 1812 (UDP)	• 67 (UDP) • 68 (UDP) • 443 (TCP) • 636 (TCP) • 1812 (UDP)

Unified Communications Management IPsec ISSS management interface page

From the Unified Communications Management main navigation menu, click **Network > CS 1000 Services > IPsec**. The IPsec for Intra System Signaling Security page appears, as shown in the following figure.

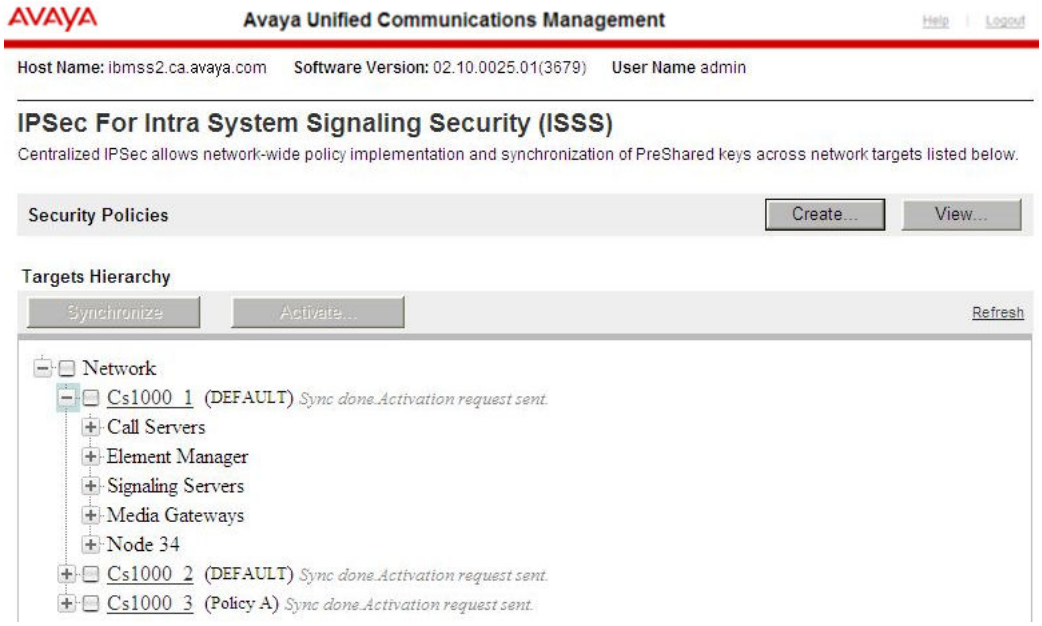


Figure 2: IPsec for Intra System Signaling Security page in UCM

The tree view on the ISSS summary page shows the target hierarchy of all CS 1000 and CS 1000 HS systems available in the security domain. One or more CS 1000 or CS 1000 HS systems can be selected from the tree for Synchronization and Activation. Each element which corresponds to a CS 1000 system or CS 1000 HS system is a hyperlink which uses the detailed configuration and status for that system. ISSS security policies can be created or viewed using the Create or View buttons on the ISSS summary page.

Warning:

If you configure a network element as Enabled, it must communicate using IPsec as defined by the current level (OPTI or FULL). If you configure the element as Disabled, it continues to

communicate with the other elements without IPsec protection. This is not recommended as it may create a security vulnerability. Do not run the scanner on the ELAN directly.

The Configuration and status for system page contains two main sections, the Configuration and Status area and the Targets table, as shown in the following figure.

- The Configuration and Status area displays the Policy Name, the security level as found in the select policy, synchronization status of the system. Synchronization or Activation is also performed from this page. You can Save and Synchronize or Activate on the systems after a change in the configuration.
- The Targets table lists all targets belonging to the selected CS 1000 system for which the IPsec configurations are applicable. You can modify targets by clicking the Add, IPsec Required, IPsec Not Required, or Remove buttons.

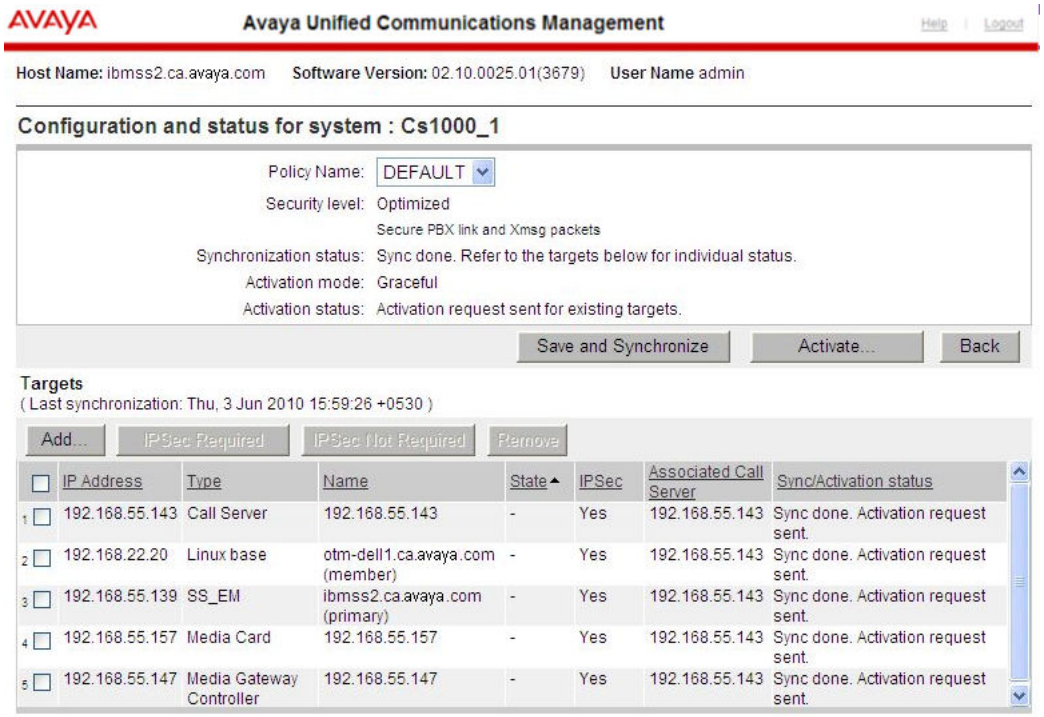


Figure 3: Configuration and status for system page

The following table shows the Target table items and a description of the information each column contains.

Table 21: IPsec Targets table item descriptions

Item	Description
IP Address	ELAN IP of the IPsec target.
Type	Type of the IPsec target.
Name	Friendly name of the IPsec target.

Table continues…

Item	Description
State	Displays the state of the target, where: • NEW: the target has not been synchronized • DELETED: the target had been synchronized, but was deleted • "_": the target has previously been synchronized
IPsec	Displays whether IPsec is required or not required for a target. This represents the locally saved status for the target; changes to the IPsec status of targets do not appear until the synchronization and activation process has been completed.
Associated Call Server	The Call Server to which the target is associated.
Sync/Activation status	Displays the current or last sync/activation status. The status messages are: • **Synchronizing**: This message displays if synchronization is in progress. • **Sync done. Activation required** : This message displays after synchronization completes but activation has not yet taken place. • **Sync done. Activation request sent**: This message displays after synchronization and activation completes. • **Sync done. Activation request failed**: This message displays after synchronization completes but activation has failed. • **Sync done. Sending activation request**: This message displays after synchronization completes and activation is in progress. • **Sync failed**: This message appears if synchronization fails due to system or network problems.

Important:

The following restrictions apply to ISSS/IPsec:

- To use ISSS, all components must be running Communication Server 1000 Release 6.0 or greater.
- On VxWorks-based devices, IPsec applies only to the ELAN.

ISSS synchronization and activation

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

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

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

IPsec configuration

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

Prerequisites

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

Configuring ISSS for a new installation

After a new installation, when the IPsec for Intra System Signaling Security (ISSS) page is loaded for the first time the default policy is not configured. All CS 1000 and CS 1000 HS systems available on the UCM security domain are shown in the Targets Hierarchy tree view.

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

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

   The IPsec for Intra System Signaling Security (ISSS) page displays.
2. Configure the default security policy.

   For the procedure to configure or edit security policies, see Configuring the default security policy on page 72.
3. (Optional) Assign custom security policy to the desired system. ISSS settings can be customized for individual system by assigning security policy different from the default policy.

   For the procedure to create new security policies, see Assigning a custom created security policy to a system on page 74
4. (Optional) Associate manual targets to required systems. Manual targets are not automatically associated to CS 1000 or CS 1000 HS systems. If no manual targets are required, please skip this step.

   For the procedure to add a manual target, see Manual IPsec targets on page 76.
5. (Optional) Disable IPsec for any desired member targets of the CS 1000 systems. If IPsec is required for all targets, you can skip this step.

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

   - The target is not configured for IPsec or is not capable of communications using IPsec.

- New or replacement elements, such as Gateway Controllers and Media Cards that require a firmware upgrade before being able to register with UCM, may need to have IPsec disabled until they are able to register with the UCM security domain and obtain the ISSS configurations.

For the procedure to enable or disable IPsec for targets, see Enabling or disabling IPsec for a target on page 78.

6. Synchronize IPsec configuration settings on systems.

   For the procedure to synchronize settings to system member targets, see Synchronizing IPsec configuration settings on page 79.

7. Activate the IPsec configuration on systems.

   For the procedure to activate the IPsec configuration, see Activating the IPsec configuration settings on page 80.

Important:

During the activation of ISSS parameters, there may be temporary disruption to internal system messaging. As a result, various system events may be reported and service may be impacted. The system recovers from these interruptions once activation is complete on all communicating members. The impact of activation depends on the type of change and the options selected, as indicated below.

When modifying ISSS levels on a Communication Server 1000 system or activating changes in forced mode, you should schedule the activation during a maintenance window for all affected call servers. In the worst case scenario, disruptions may last for several minutes, with the duration generally increasing with the number of members in the UCM security domain. Typical disruptions should be less than one minute.

The activation of changes within a specific ISSS level that are requested with graceful activation, including the addition or removal of targets, enabling or disabling of ISSS for targets, and changes to the PSK, have minimal impact on system operations and are isolated to the new or modified targets. This is the normal mode of operation once the ISSS level has been configured for a Communication Server 1000 system.

Note:

Temporary interruptions can occur not only when using forced activation mode, but also with graceful mode. This can be represented by the ELAN link going down and an outage of related services until all the elements are properly synchronized. The probability of such an interruption increases in accordance with the number of targets in the system.

Configuring the default security policy

The ISSS security parameters are configured into a security policy. Each security policy contains a PSK and security level. The policies can be assigned to one or more CS 1000 or CS 1000 HS systems for configuring the ISSS parameters.

Click View on the ISSS summary page to view the available policies on the Security policies page. On a freshly installed server, the default policy must be configured before performing any ISSS operations. By default, all CS 1000 and CS 1000 HS systems are associated to the default policy.

Configure the default security policy.

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

   The IPsec For Intra System Signaling Security (ISSS) summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Security Policies section, click **View** to view the existing policies.

   The Security policies page appears, as shown in the following figure.

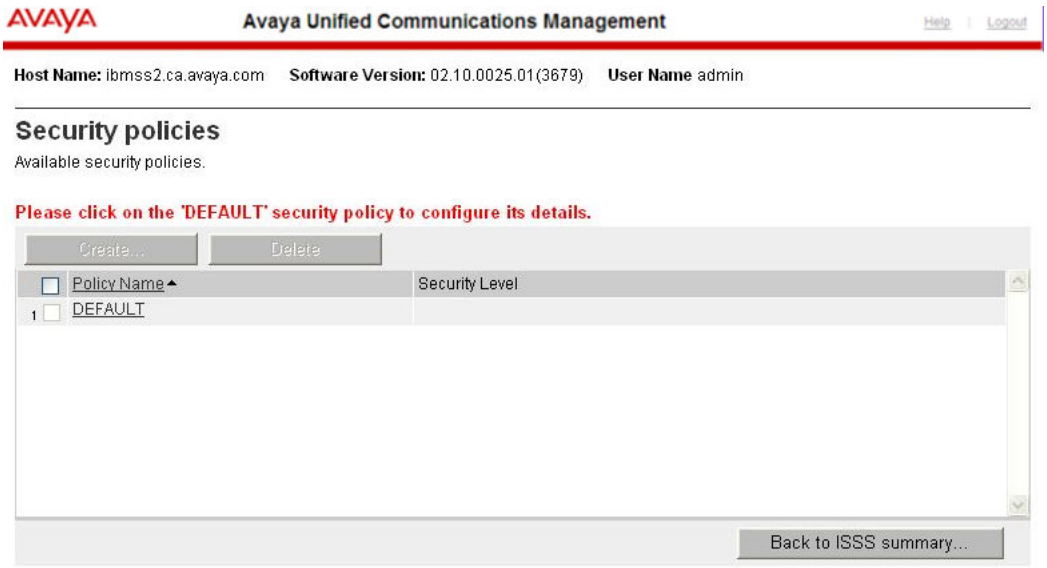


Figure 4: Security policies page

4. Click the name of the default policy.

   The Edit Security Policy page appears, as shown in the following figure.

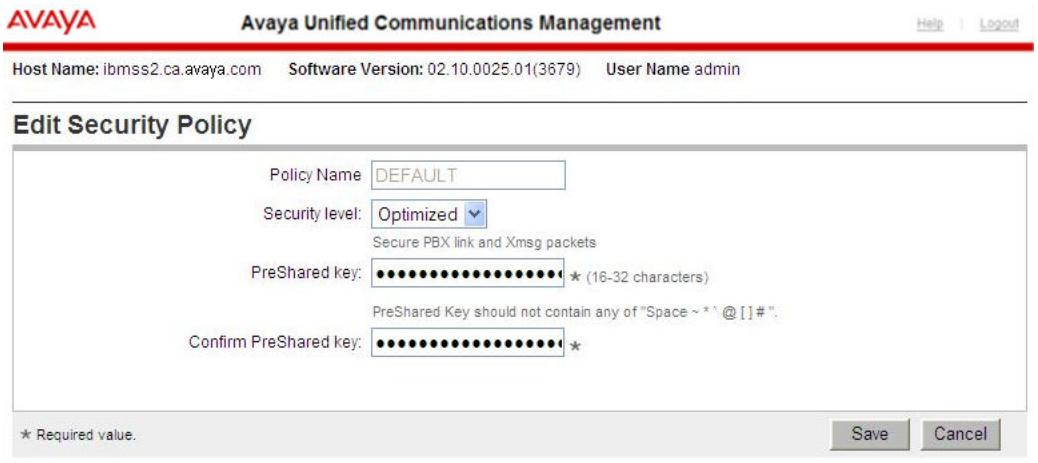


Figure 5: Edit Security Policy page

5. Select the desired Security Level and enter the appropriate PreShared key. You must enter the PreShared key again to confirm, as shown in the preceding figure.

6. Click **Save** or click **Cancel** to return to the Security policies page.
7. On the Security policies page, click Back to ISSS summary.

Assigning a custom created security policy to a system

One or more CS 1000 systems can be assigned with different ISSS parameters other than the one specified in the DEFAULT security policy. You can create additional security policies and assign it to one or more systems. Use the following procedure to create a new security policy and assign it to a system.

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

   The IPsec For Intra System Signaling Security (ISSS) summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Security Policies section, click Create.

   The Create Security Policy page appears.
4. In the Policy Name field, type a policy name
5. In the Security level field, choose Optimized or Full from the list.
6. In the PreShared key field, enter the appropriate PreShared key and in the Confirm Preshared key field, enter the PreShared key again to confirm.
7. Click Save.

   The Security Policies page appears.
8. Click Back to ISSS summary page.

   The IPsec For Intra System Signaling Security (ISSS) summary page appears.
9. From the Targets Hierarchy section, select the system to which the newly created policy should be assigned.

   The Configuration and Status for system page appears.
10. In the Policy Name field, select the required policy from the list.
11. Click Save and Synchronize. Wait until the operation completes.
12. Click Activate. Wait until the operation completes.

Editing an existing security policy

Edit an existing security policy.

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

   The ISSS summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Security Policies section, click View to view the existing policies.

   The Security policies page appears, as shown in the following figure.

Figure 6: Security policies page

4. Click the name of the policy to edit.

   The Edit Security Policy page appears, as shown in the following figure.

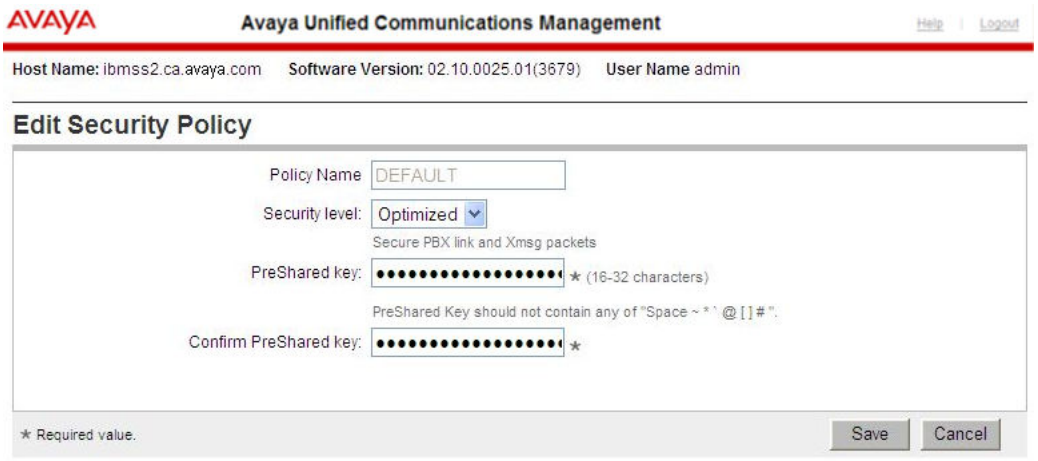


Figure 7: Edit Security Policy page

5. In the Security level field, choose Optimized or Full from the list.
6. In the PreShared key field, enter the appropriate PreShared key and in the Confirm Preshared key field, enter the PreShared key again to confirm.
7. Click Save or Cancel to return to the Security policies page.

   The Security Policies page appears.

   Important:

   After changing the policy details, the systems where the policy is associated need to be synchronized and activated for the changes to take effect.

8. Click Back to ISSS summary.

9. From the Target Hierarchy tree view, select the check box of the systems assigned with the edited policy, and click Synchronize. Wait until the operation completes.
10. Select the systems synchronized in the preceding step and click Activate. Wait until the operation completes.

Deleting an existing security policy

Prerequisites:

- Ensure the security policy is not assigned.
- The default security policy cannot be deleted.

Use the following procedure to delete an existing policy.

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

   The ISSS summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Security Policies section, click View.
4. Select the check box beside the policies to delete and click Delete.
5. Click Back to ISSS summary page.

Manual IPsec targets

Manual targets are targets that are not registered to the UCM security domain. These targets have to be manually defined and associated to required CS 1000 and CS 1000 HS systems.

Adding a new manual IPsec target in UCM

Use the following procedure to define a new manual target in UCM.

1. Log on to the UCM primary security server.
2. From the navigation tree, select **Network > Elements**.
3. Click **Add**.

   The Add New Element page appears.
4. In the Name and Description fields, enter an Element name and description.
5. In the Type field, select Non CS1000 Manual Device from the list.
6. Click Next
7. Obtain the following information and enter it into the appropriate fields:
   - IP address 1: the IP address of the target

Note:

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

- IP address 2: the second network interface of the manual target, if available.

8. Click Save.

   The Elements page appears. The target is listed in the elements table.

Associating a manual IPsec target to a system

Use the following procedure to associate manual targets that are available in UCM to a system.

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

   The IPsec for Intra System Signaling Security (ISSS) summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68
3. In the Targets Hierarchy section , click the system name to associate the manual target.

   The Configuration and status for system page appears.
4. In the Targets section, click Add.

   The Associate Manual Target to System page appears, as shown in Figure 8: Associate Manual Target to System page on page 77.
5. Choose an element from the Select element list, and select the **IPsec required** check box, as shown in the following figure.

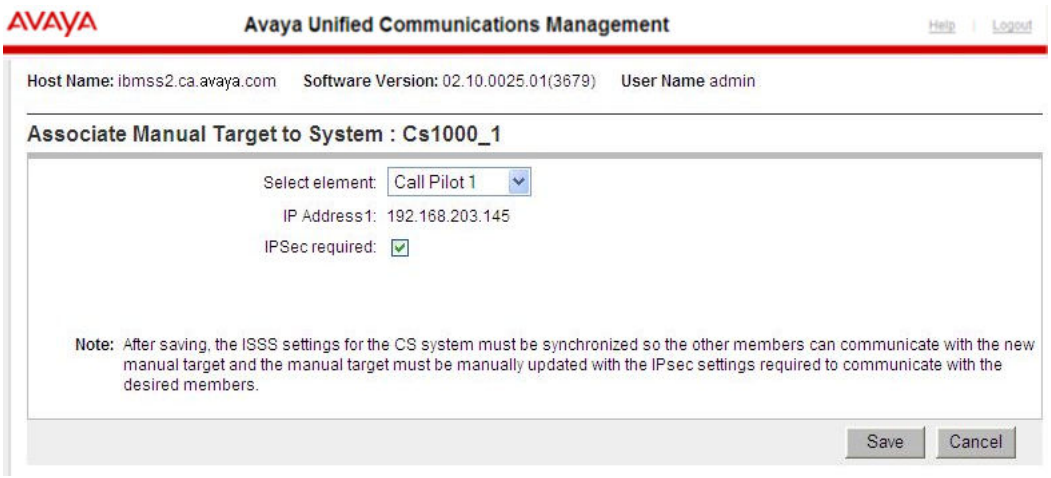


Figure 8: Associate Manual Target to System page

Note:

Clearing the IPsec required check box allows the target to communicate without IPsec security to other elements in the system.

6. Click Save to save the association.

   The Configuration and status for system page appears. The manual target State is listed as New in the Targets table.

Note:

After associating the manual target, the system must be synchronized and activated so that the new manual target information is passed to all UCM targets.

Removing a manual target

Use this procedure to remove a manual target.

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

   The ISSS summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Targets Hierarchy section, click on the system name for the system where the manual link is being removed.

   The Configuration and Status for system page appears, as shown in Figure 3: Configuration and status for system page on page 69.
4. From the Targets table, select the check box for each manual target to be removed.
5. Click **Remove**.
6. Click **Save and Synchronize**. Wait until the operation completes.
7. Click Activate. Wait until the operation completes.
8. Click the IPsec link to get the latest synchronization status.

Note:

If a manual target is in the "New" state and it is removed, the system does not need to be Synchronized or Activated.

Enabling or disabling IPsec for a target

Use the following procedure to enable or disable IPsec for a target.

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

The ISSS summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.

3. From the Targets Hierarchy section, click on the system name for the system which contains the target.

   The Configuration and Status for system page appears, as shown in Figure 3: Configuration and status for system page on page 69.

4. In the Targets table, select the check boxes beside the names for the targets where you want to enable or disable.
5. To enable the selected targets, click **IPsec Required**.

   OR

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

   Note:

   Depending on the current IPsec status of the selected targets, the IPsec Required or IPsec Not Required button is disabled.

   Note:

   After enabling or disabling IPsec for any targets, you must initiate the synchronization and activation process.

Synchronizing IPsec configuration settings

Use this procedure to synchronize the IPsec configuration to the associated member elements.

Manually synchronize the settings after making any change to the system configuration:

- Adding or removing elements from CS 1000 or CS 1000 HS system.
- Enabling or disabling IPsec for a target.
- Adding or removing manual targets.
- Changing or updating the associated security policy.

1. Log on to the UCM primary security server.
2. From the navigation tree, select **Network > CS 1000 Services > IPsec**, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68.
3. From the Targets Hierarchy section, select the check boxes beside the systems names for the targets that need synchronizing.
4. Click **Synchronize**.

   The synchronization process initiates. A synchronization indicator is shown next to the system until the operation completes, as shown in the following figure.

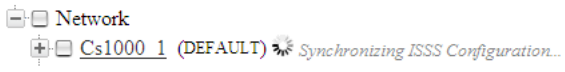


Figure 9: Synchronization process indicator

Note:

Synchronization of IPsec settings must be followed by the Activation process.

Activating the IPsec configuration settings

Use this procedure to activate the last synchronized IPsec configuration settings. You must activate for the configuration settings to take effect.

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

   The ISSS summary page appears, as shown in Figure 2: IPsec for Intra System Signaling Security page in UCM on page 68
3. From the Targets Hierarchy section, select the check box beside the system names for the systems that need Activation.

   The IPsec Activation details page appears, as shown in the following figure.
4. Click **Activate**.

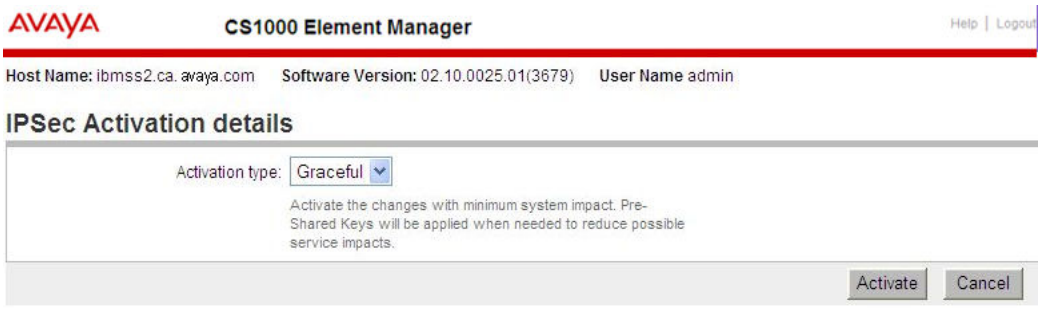


Figure 10: IPsec Activation details page

5. From the **Activation type** list, select the activation mode. You can choose Graceful or Forced.
6. Click **Activate**.

   The Activation process initiates. An activation indicator is shown next to the system until the operation completes, as shown in the following figure.

Figure 11: Activation process indicator

Note:

If a new element, such as a Gateway Controller or Media Card is added to the security domain, perform the activation of the updated ISSS parameters in Graceful mode to minimize any potential system interruptions. If activating ISSS in Graceful mode, only the IP traffic of the updated elements are impacted. All existing security associations are

maintained and only the rules for the updated members are deleted or added on each of the other elements.

Enabling IPsec for Media Gateway Controller and Media Cards configured with alternate call servers

Use the following procedure to configure ISSS for a Media Gateway Controller (MGC) or Media Card that is configured with alternate call servers.

Important:

This procedure is required only when the alternate call servers associated to the MGC or Media Card belong to a Communication Server 1000 system other than the primary call server. If the alternate call servers belong to the same Communication Server 1000 system as the primary call server, you can Synchronize and Activate on that system for enabling ISSS on the MGC and Media Card.

Prerequisites:

- Configure the Media Gateways and Media Cards through Element Manager in UCM.

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

   The IPsec for Intra System Signaling Security (ISSS) page appears.
3. From the Targets Hierarchy section, click the system name of CS 1000 or CS 1000 HS system which contains the primary call server of the MGC or Media Card.

   The Configuration and status for system page appears, as shown in the following figure.

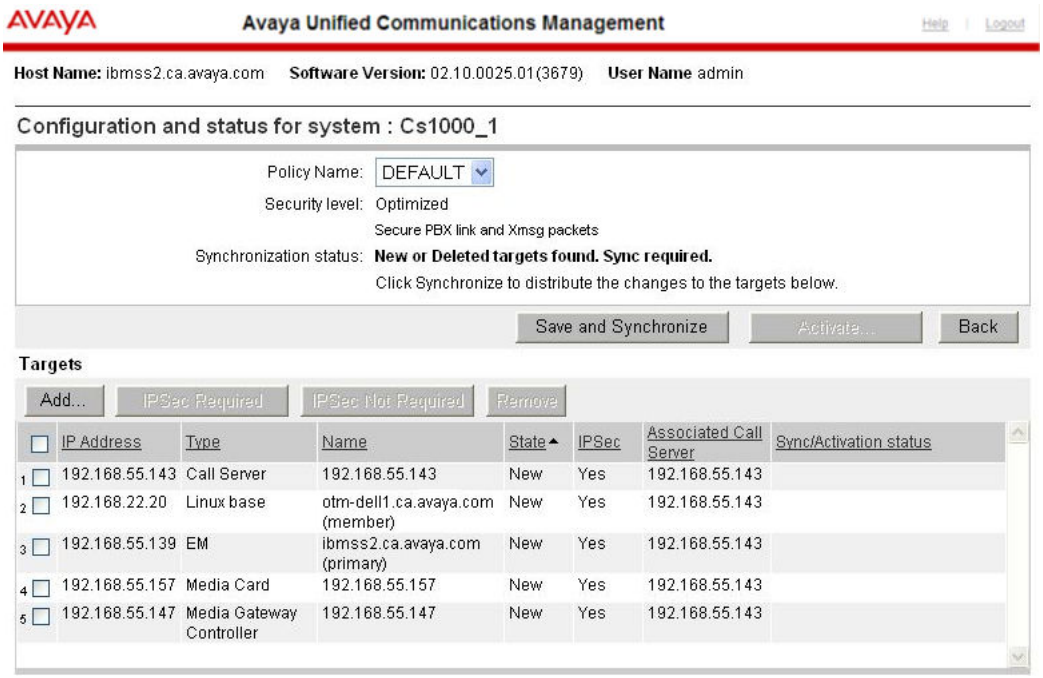


Figure 12: Configuration and status for system page

4. (Optional) Enable or disable ISSS for the MGC or Media Card. For the procedure to enable or disable IPsec for individual targets, see Enabling or disabling IPsec for a target on page 78.
5. (Optional) In the Policy Name field, choose the required policy from the list.
6. Click Save and Synchronize. Wait until the operation competes.
7. Click Activate. Wait until the operation completes.
8. Click Back.
9. From the Targets Hierarchy section, click the system name of the CS 1000 or CS 1000 HS system that contains the alternate call server of the MGC or Media Card.

   The Configuration and Status for system page appears, as shown in the following figure. The MGC or Media Card targets configured as alternate call servers appear in colored text.

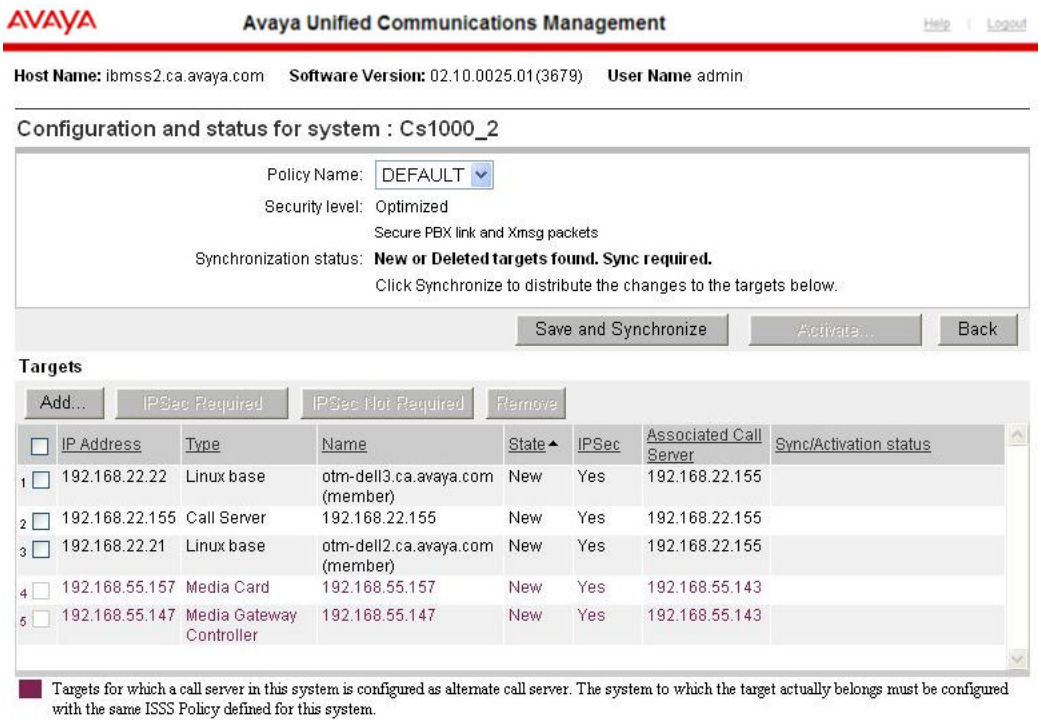


Figure 13: Configuration and status for system page identifying alternate call servers

10. In the Policy Name field, choose the required policy from the list. Use the same policy name as chosen in 5 on page 82.
11. Click Save and Synchronize. Wait until the operation completes.
12. Click Activate. Wait until the operation completes.

Note:

The CS 1000 systems containing the primary and alternate call servers should be using the same security policy.

Note:

The procedure for Enabling IPsec for Media Gateway Controller and Media Cards configured with alternate call servers is required only when the alternate call servers associated to the MGC or Media Card belongs to a CS 1000 system that is different than the system of the primary call server. If the alternate call servers belong to the same CS 1000 system as of the primary call server, you can synchronize and activate on that system to enable IPsec on the MGC and Media Card.

Important:

The MGC or Media Card must be reregistered to the security domain after making any configuration changes. Reregistering ensures ISSS management receives the configuration changes and ISSS configuration is adjusted. After reregistering, perform synchronization and activation on the CS 1000 systems which contains the associated call servers. All members of the system receive the updated configuration.

Viewing the Preshared Key (PSK)

VxWorks-based systems

To view the PSK on a VxWorks Call Server:

1. Log into the Call Server using PDT mode and navigate to `/e/sdm`.
2. At the prompt, enter the following command: `cat ipsec.xml`.

Linux-based systems

To view the PSK on a Linux system:

1. Log in as a root user and navigate to `/opt/nortel/base/ipsec`.
2. At the prompt, enter the following command: `cat psk.txt`.

Chapter 7: Certificate Management

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

- Prepare the system for certificate management on page 85
- CA management on page 86
- Certificate creation and management on page 92

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

For more information about public-key and private-key certificate concepts, Web SSL, and SIP TLS on Communication Server 1000, see Public-key certificate concepts on page 24.

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

Prepare the system for certificate management

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

Avaya recommends that you perform certificate management from the Unified Communications Management primary security server that is running Element Manager. For certificate management purposes, the Unified Communications Management element management table must contain an entry for each Communication Server 1000 system and Signaling Server. You must add the Communication Server 1000 elements and configure ISSS before you perform certificate management. For more information about adding system elements and configuring ISSS, see IPsec configuration on page 71. You must also add each Communication Server 1000 system to the Unified Communications Management elements table, and add each signaling server as separate elements.

CA management

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

Private CA Configuration

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

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

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

Use the following procedure to access the primary security server.

Accessing UCM on the primary security server

1. In the Web browser address field, type https://<fqdn>, where <fqdn> is the fully qualified domain name of the primary security server.

   If the certificate is not installed in the Web browser, a Security Alert window appears, stating that the private CA installed on the primary security server is not in the trusted CA list in the Web browser.

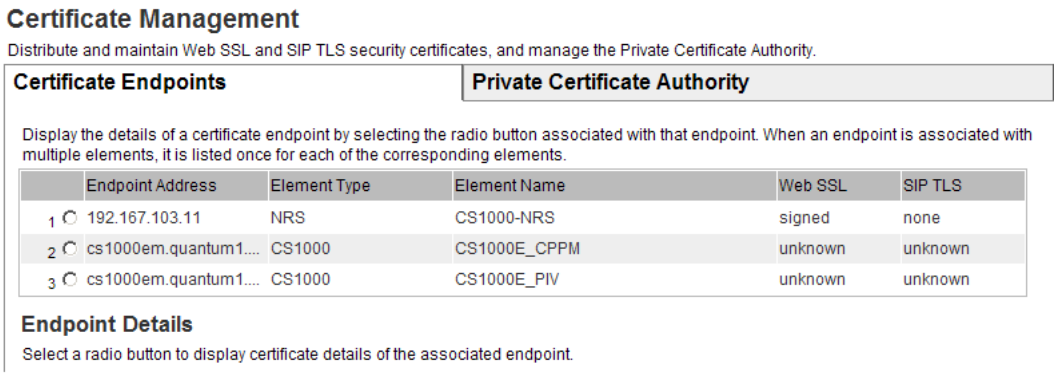
2. If the CA is not in the trusted list Security Alert window appears, add the private CA to the trusted CA list in the Web browser using Installing a certificate into the trusted CA list in the Web browser on page 88.
3. Click Yes to proceed.

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

Viewing private CA details

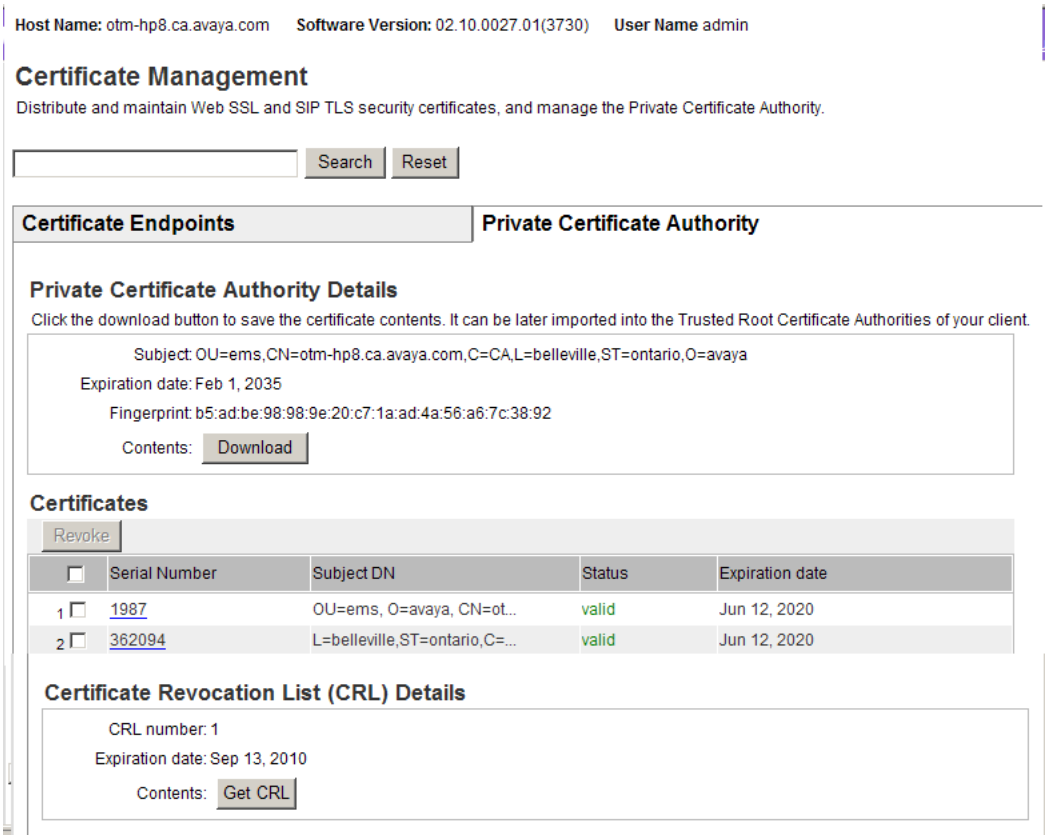
1. Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2. Click Security > Certificates.

   The Certificate Management page appears.



3. Click the Private Certificate Authority tab.

   The Private Certificate Authority Details page appears.



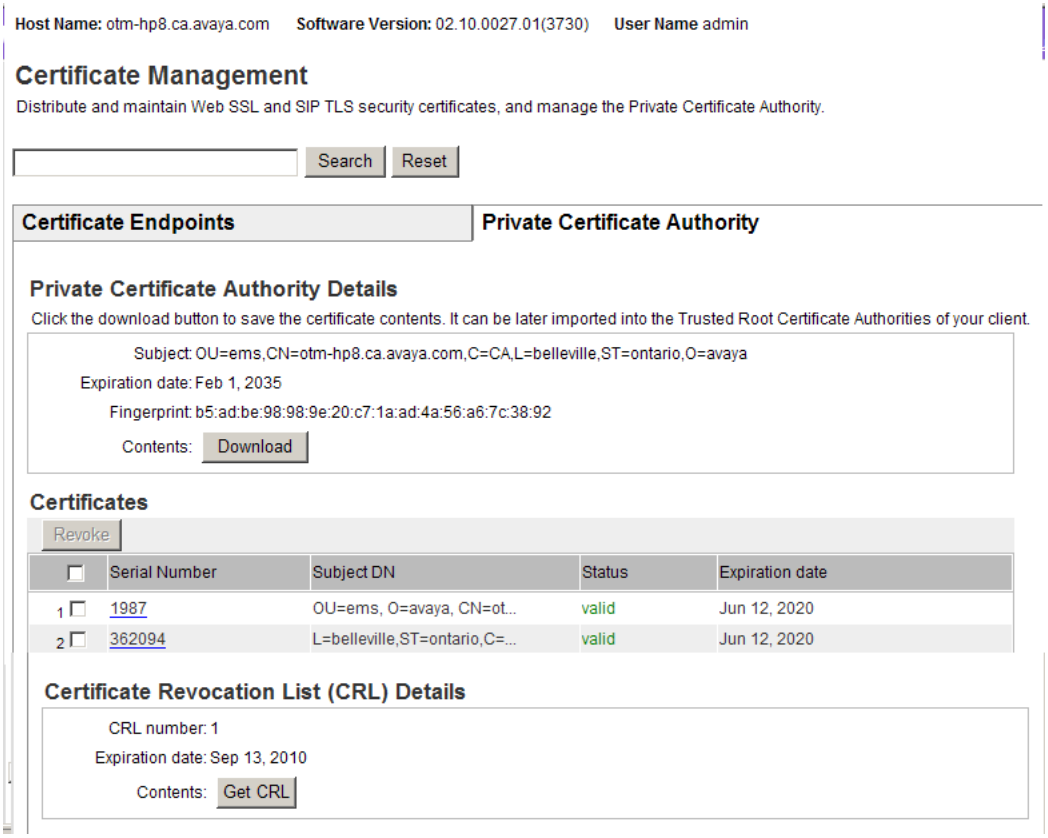
Use the following procedure to add the private CA to the trusted CA list in the Web browser.

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

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

   The Certificate Management page appears.
3. Click the Private Certificate Authority tab.

   The Private Certificate Authority Details page appears, as shown in the following figure.



4. Click **Download** to download the certificate.
5. Follow the prompts in the wizard to install the certificate into the trusted CA list of the Web browser.

Add a CA to an endpoint

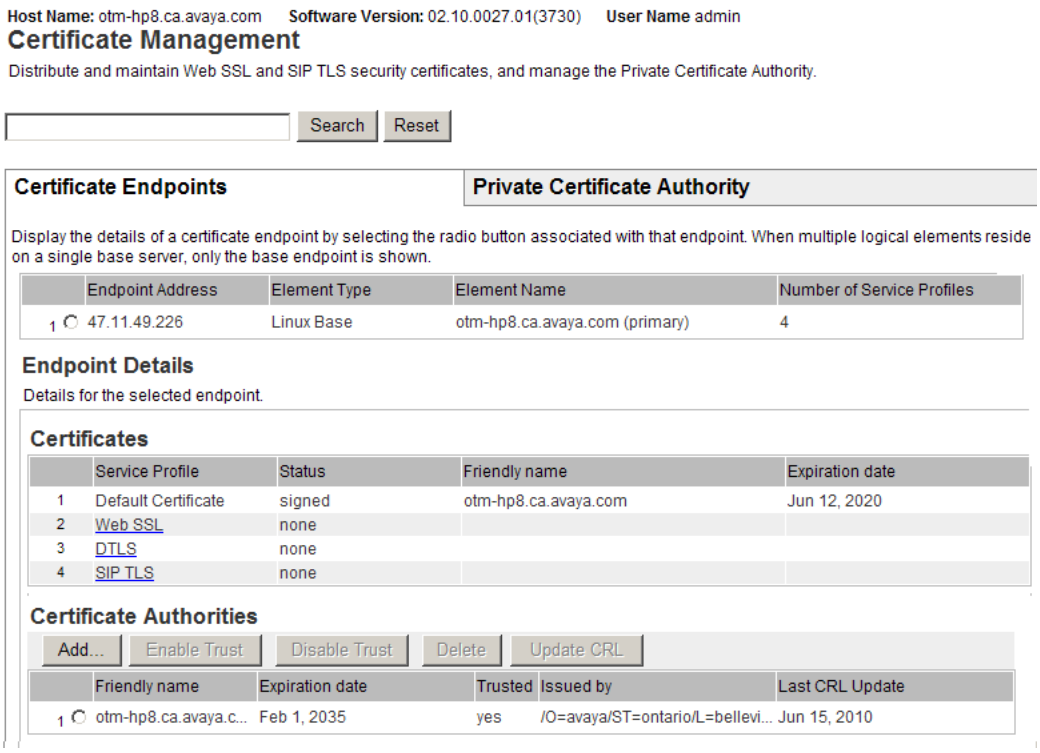
Use the following procedure to add a CA to a selected endpoint by using Unified Communications Management.

Adding a CA to an endpoint

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

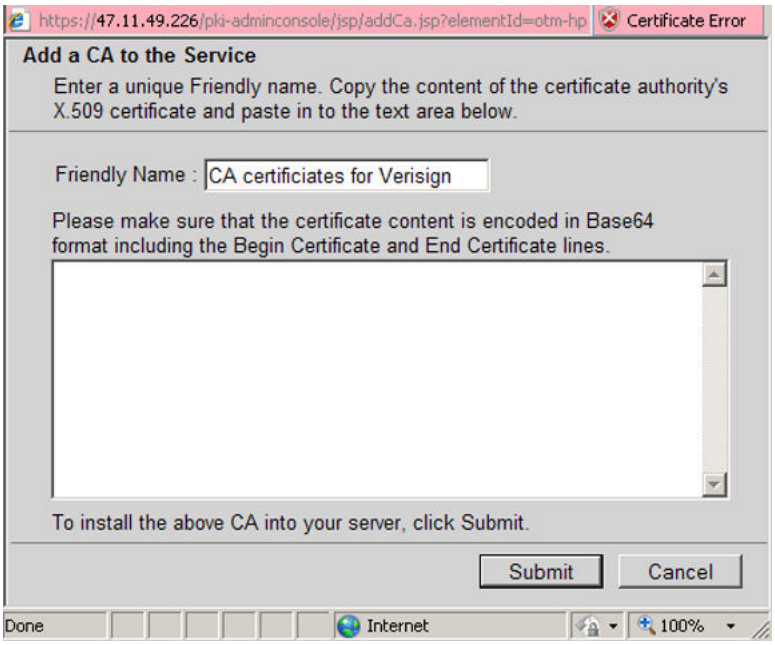
2. Click Security > Certificates.

   The Certificate Management page appear, as shown in the following figure.



3. In the Certificate Endpoints pane, select the radio button next to an endpoint.
4. In the Certificate Authorities pane, click Add.

   The Add a CA to the Service window appears.



5. Type a name in the Friendly Name field.
6. Copy the contents of the X.509 certificate, which is provided by the CA in a privacy-enhanced electronic mail (PEM) text file.
7. In the Add a CA to the Service window, click in the text box, and press ctrl-v to paste the certificate text.
8. Click Submit.
9. Restart the server that you changed in this procedure.

   The changes take effect only after the server restarts.

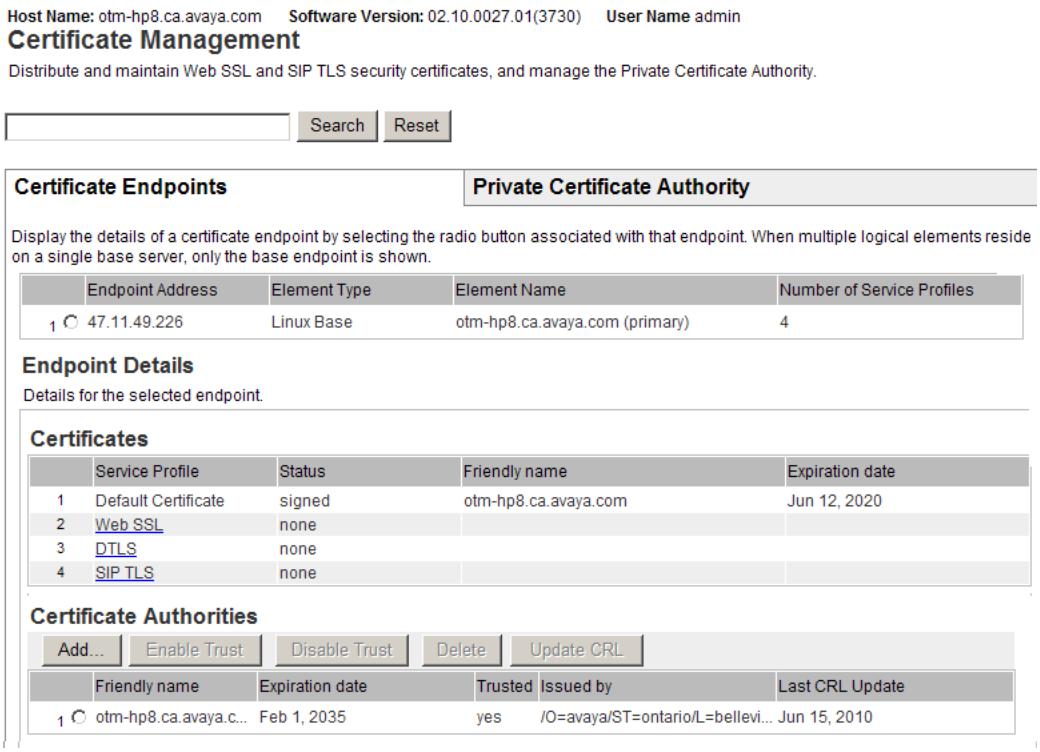
Change the trust status of an endpoint

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

Changing the trust status of an endpoint certificate

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

   The Certificate Management page appears.



3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure.
4. In the Certificate Authorities pane, select a CA.

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

   Enable Trust OR Disable Trust .

   The modified trust status appears on the page.
6. Restart the server that you changed in this procedure.

   The changes take effect only after the server restarts.

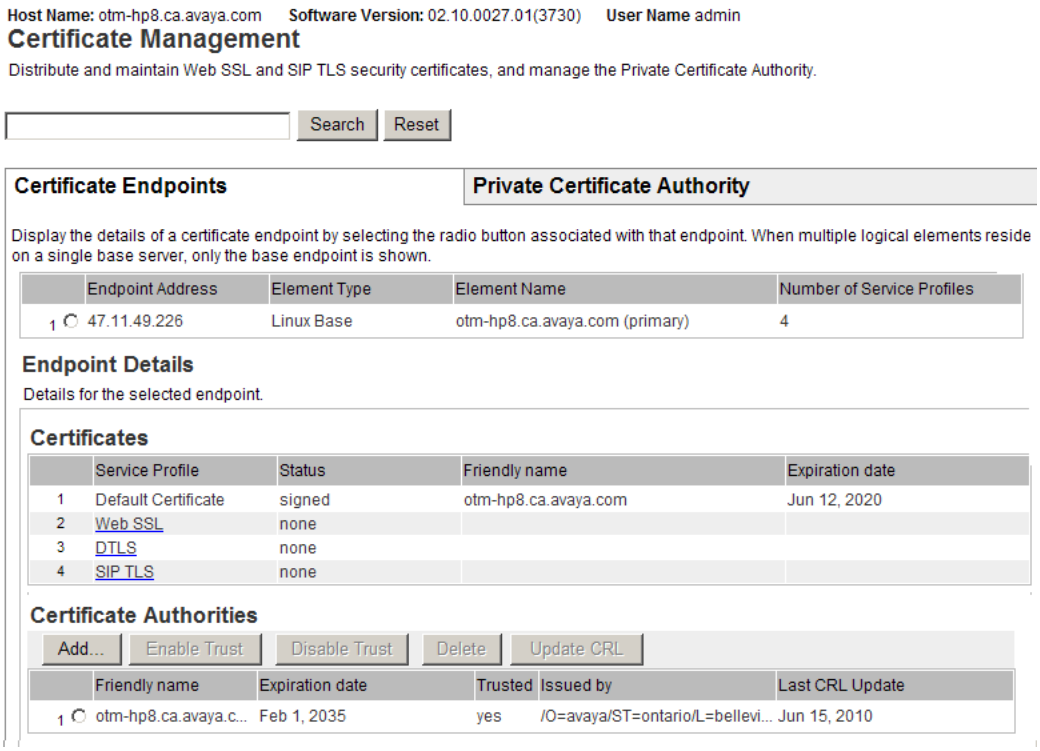
Delete a CA

Use the following procedure to delete a CA.

Deleting a CA

1. Log on to the UCM primary security server using an account that has Security Administrator privilege.
2. Click Security > Certificates.

   The Certificate Management page appears.



3. In the Certificate Endpoints pane, select the radio button next to an endpoint.
4. In the Certificate Authorities pane, select a CA.
5. Click **Delete**. A confirmation window appears.
6. Click OK.
7. Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

Certificate creation and management

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

You can use the Unified Communications Management Certificate Management Wizard to complete the following tasks:

- 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

Important:

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

For more information about the different status types for Web SSL and SIP TLS certificates, see Table 22: Status types for certificate endpoints on page 92.

Table 22: 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.

Table continues…

Status type	Description
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.

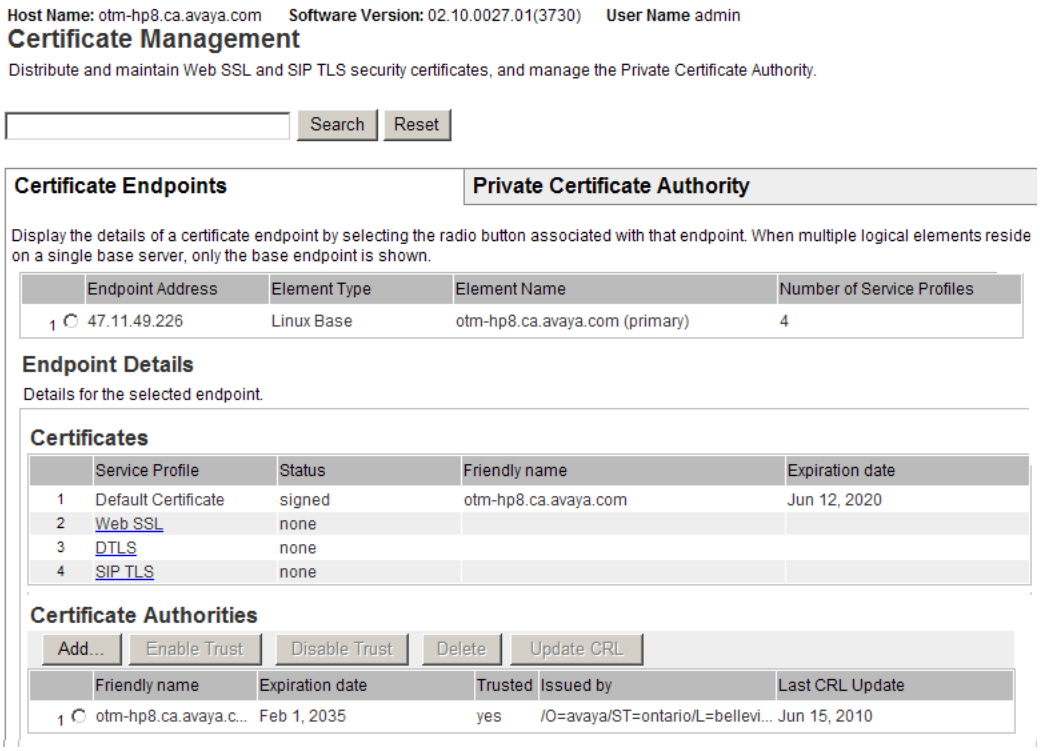
Certificate information

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

Viewing certificate details for an endpoint by using UCM

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

   The Certificate Management page appears.



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

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

For more information about the different status types, see Table 22: Status types for certificate endpoints on page 92.

Adding a UCM server certificate to the Web browser

When you gain access to the UCM server by using a Web browser for the first time, the system displays a security alert warning that describes the problem with the authenticity of the server certificate. You can The server certificate can be trusted; however, this warning appears each time you visit the site.

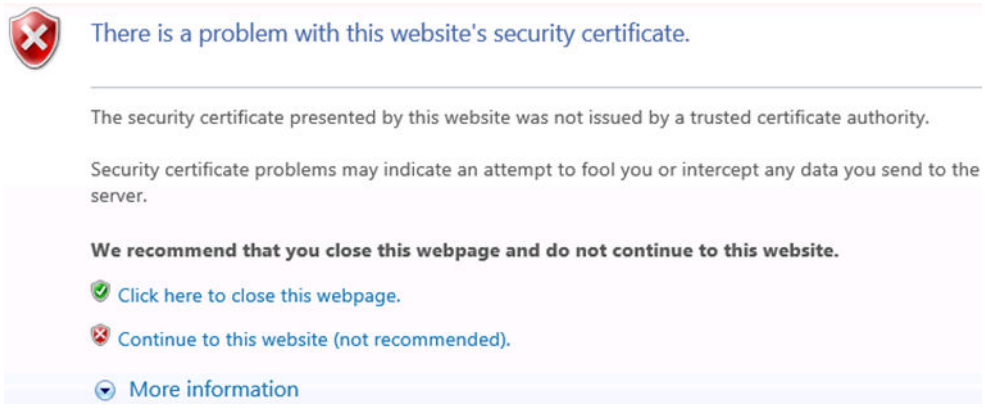
Use this procedure to add the UCM server certificate to the Web browser as a trusted certificate to prevent the warning each time you visit the site.

Adding a UCM server certificate to the Web browser

1. Perform one of the following:
   - For Internet Explorer 6.0, when the system displays the following security alert, click **View Certificate** and go to 9 on page 95.

     The system displays the certificate information.
   - For Internet Explorer 7.0 and later, when the system displays following security warning message, click **Continue to this website (not recommended)**:

2. Click **Tools** > **Internet Options**.
   a. Click **Security** > **Trusted sites** > **Sites**.

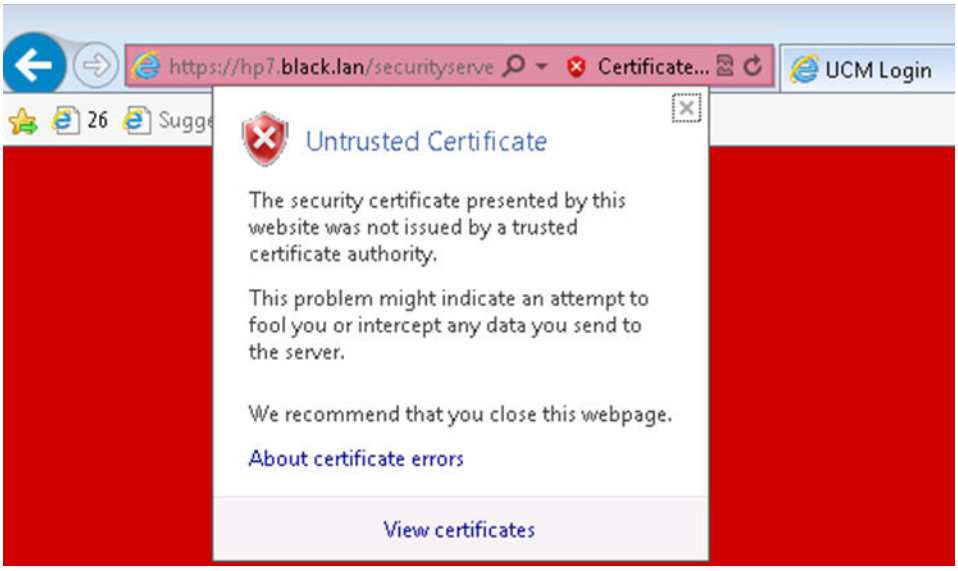
b. Confirm the URL matches, and click **Add**.
c. Click **Close**.

3. Click **OK**.

   The system closes the Internet Options dialog box.

4. Click **Certificate Error** next to the address bar.
5. Refresh the current page.
6. When the system displays `There is a problem with this website's security certificate`, click **Continue to this website (not recommended)**.
7. Click Certificate Error in the address bar.

   The system displays the following message:



8. Click **View certificates**.

   The system displays the Certificate window.

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

   The CA certificate is represented at the top of the hierarchy. Usually, the certificate has a red check mark to indicate that the certificate is not yet trusted.

10. Click **View Certificate**.

    The system displays the details of the root CA certificate.

11. Click **Install Certificate**.

    The system displays the installation wizard.

12. Click **Next**.
13. Click **Place all certificates in the following store**.
14. Click **Browse**, select **Trusted Root Certification Authorities**, and click **OK**.
15. On the installation wizard, click **Next**, and click **Finish**.

16. If the system displays security warning message, click **Yes**.
17. Click **OK** to close the message box.
18. Shut down all running instances of Internet Explorer and open Internet Explorer again.

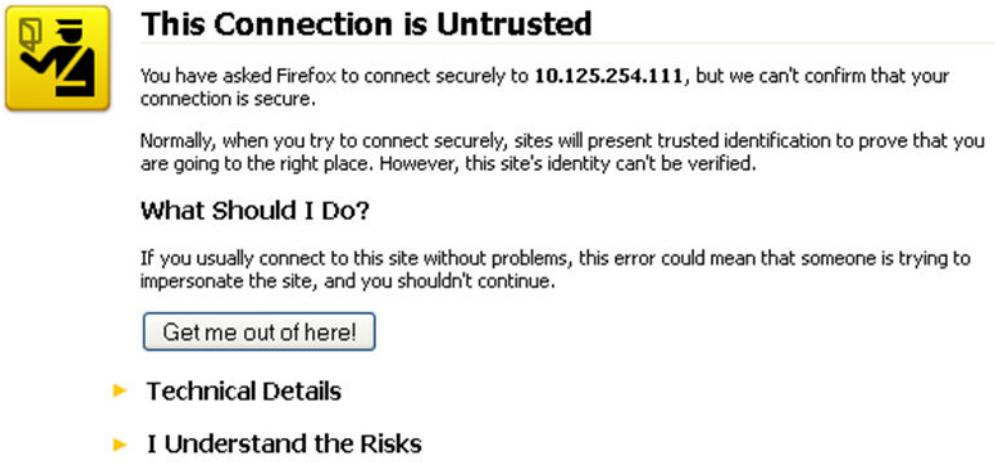
    The browser now trusts all certificates in the UCM security domain.
19. To view the trusted CA list, perform the following:
    a. Click **Tools** > **Internet Options**.
    b. Select the **Content** tab.
    c. Click **Certificates**.
    d. Select the **Trusted Root Certificate Authorities** tab.
    e. Scroll down to view the entry for the Private CA certificate.

       The entry must match the FQDN of the UCM primary security server.

Adding the UCM server certificate to the Mozilla Firefox browser

1. On the Mozilla Firefox Web browser, type the IP or FQDN of the UCM server for which you require the certificate.

   If the certificate is not installed on the Web browser, the system displays the following security alert:



2. Click **I Understand the Risks**.
3. Click **Add Exception**.

   The system displays the Add Security Exception dialog box.
4. Click **Get Certificate**.
5. Clear the **Permanently store this certificate** check box.
6. Click **Confirm Security Exception**.

7. Log on to UCM and complete the following:
   a. In the left navigation pane, click **Security** > **Certificates**.

      The system displays the **Certificate Management** Web page.
   b. Click the **Private Certificate Authority** tab.
   c. Click **Download and Save certificate to file**.
8. On the Mozilla Firefox browser, click **Tools** > **Internet Options**.
   a. In the **Advanced** tab, click **Encryption**.
   b. Click **View Certificates**.
   c. On the **Servers** tab, click **Import**.
   d. Import the CA certificate file.
   e. Scroll down to view the entry for the Private CA certificate.

      The name of the certificate must match the UCM primary security server, the **Server** field must be star (*) and the **Lifetime** field must be **Permanent**.
   f. Select the imported certificate and click **Edit Trust**.
   g. Select **Trust the authenticity of this certificate**.
   h. Click **Edit CA Trust**.
   i. Click **This certificate can identify websites**.
   j. Click **OK**.
9. Shut down all running instances of Mozilla Firefox and start Mozilla Firefox again.

   The browser now trusts all certificates in the UCM security domain.
10. Complete the following steps to view the trusted CA list of the browser:
    a. On the Mozilla Firefox 19.0 or later browser, click **Tools** > **Internet Options**.
    b. In the **Advanced** tab, click **Encryption**.
    c. Click **View Certificates**.
    d. On the **Authorities** tab.
    e. Scroll down to view the entry for the Private CA certificate.

       The name of the certificate must match the UCM primary security server.

Note:

To ensure that Web SSL works properly, you must add root CA and UCM certificate in the web browser.

Create a certificate for Web SSL signed by the private CA

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

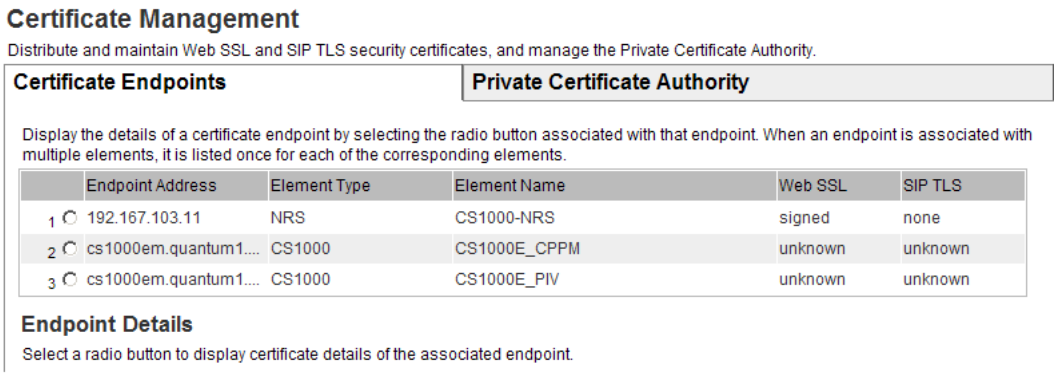
Prerequisites

- Before you create a new certificate signed by a local private CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a certificate for Web SSL signed by the private CA

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

   The Certificate Management page appears.

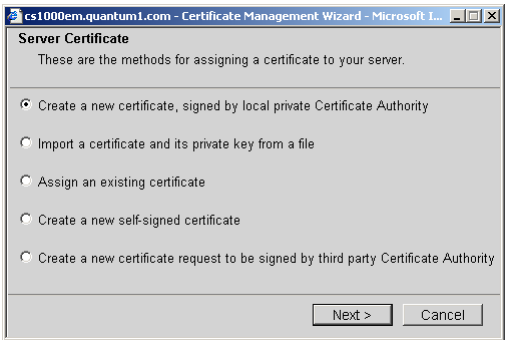


3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

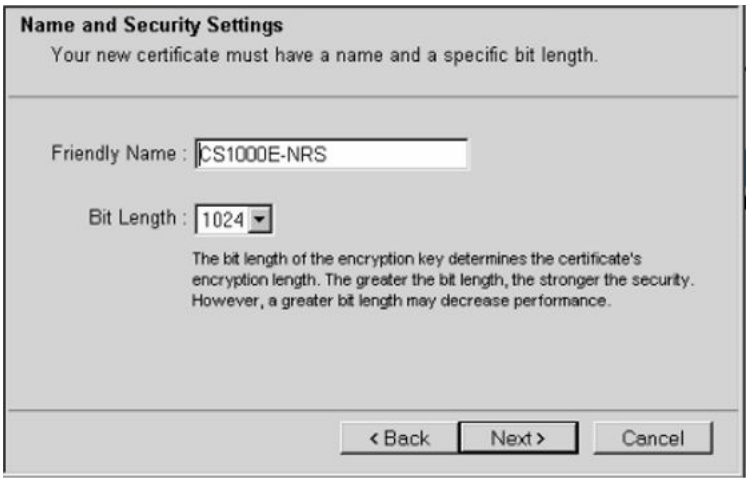
4. In the Endpoint Details pane, under Certificates, click **Web SSL**.

   The Server Certificate window appears.



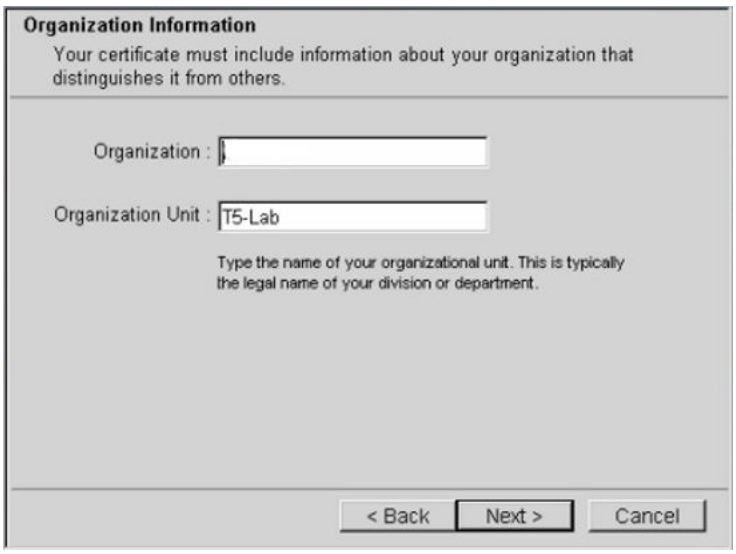
5. Select **Create a new certificate, signed by local private Certificate Authority** and click **Next**.

   The Name and Security Settings window appears.



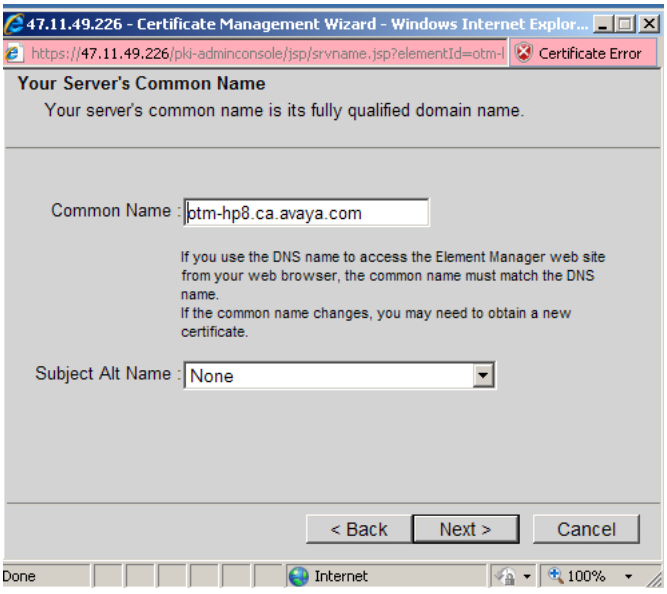
6. Type a name in the Friendly Name field.
7. Select a bit length from the **Bit length** list.
8. Click **Next**.

   The Organization Information window appears.



9. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

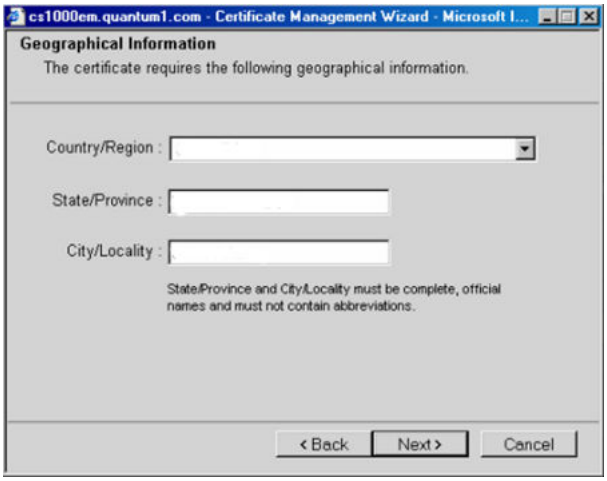
   The Your Server's Common Name window appears.



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

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

    The Geographical Information window appears.

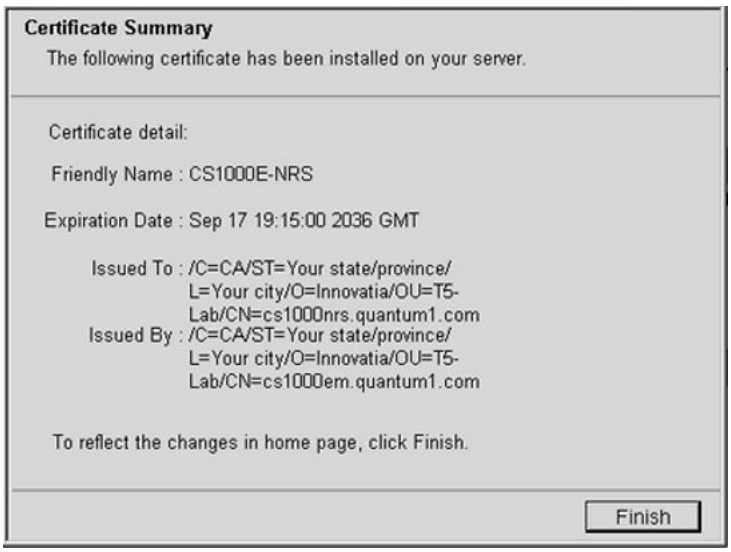


12. In the Geographical Information window, perform the following tasks:
    - In the Country/Region box, select the country from the list.
    - In the State/Province field, enter the state or province.
    - In the City/Locality field, enter the city or locality.
    - Click Next.

    The Certificate Request Summary window appears.

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

    The Certificate Summary window appears with the certificate information.



14. Click **Finish**.

    The status changes to signed.

15. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

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

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

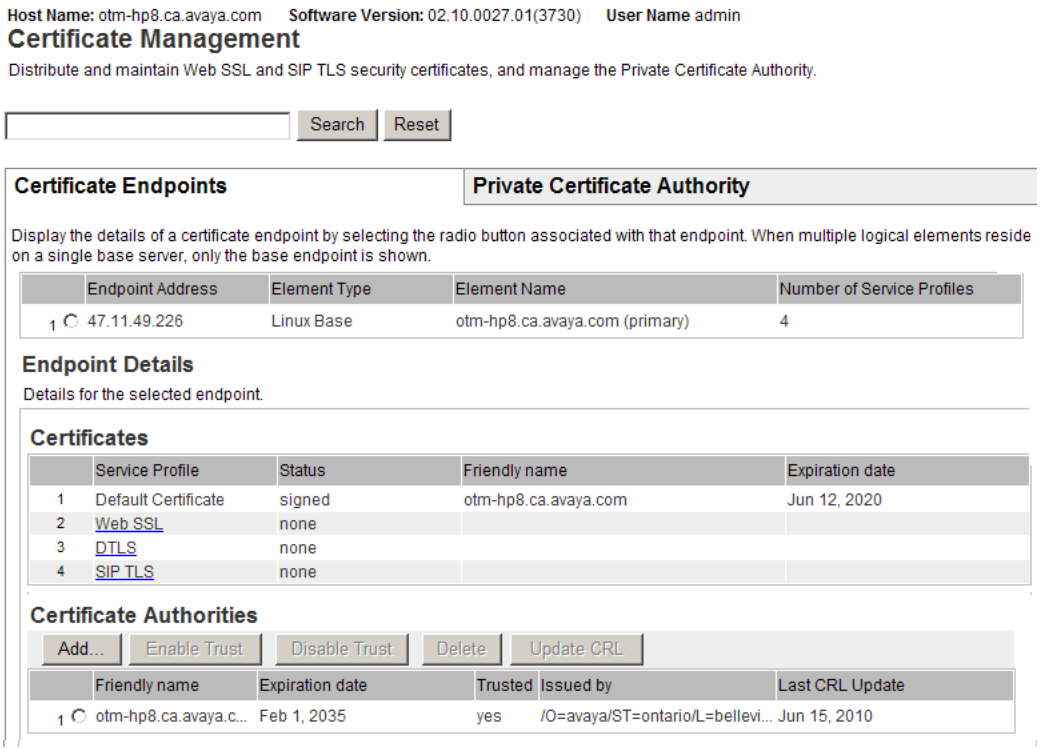
Prerequisites

- Before you create a request for a new certificate signed by a third-party CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

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

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

   The Certificate Management page appears.

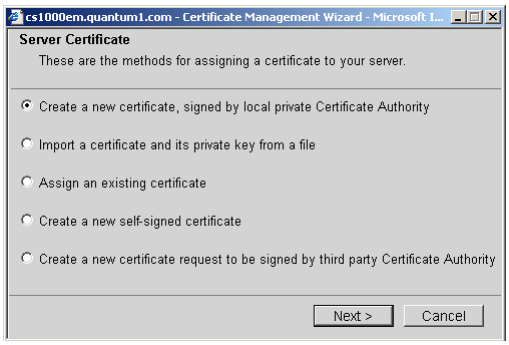


3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

   The Endpoint Details section appears.

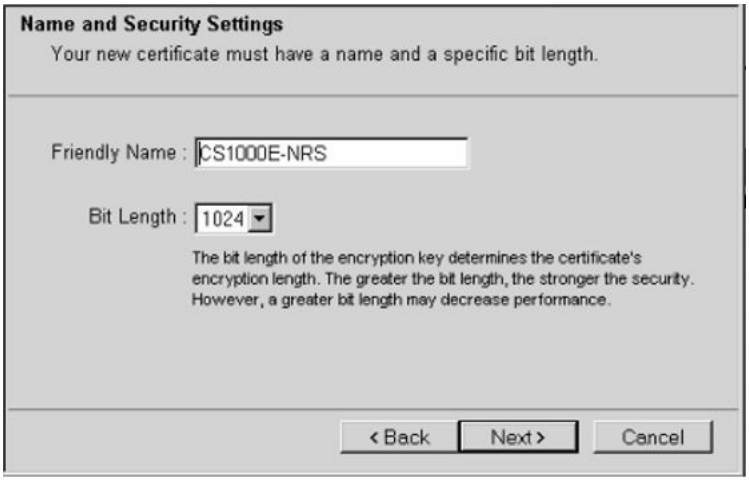
4. In the Endpoint Details pane, under Certificates, click **Web SSL**.

   The Server Certificate window appears.



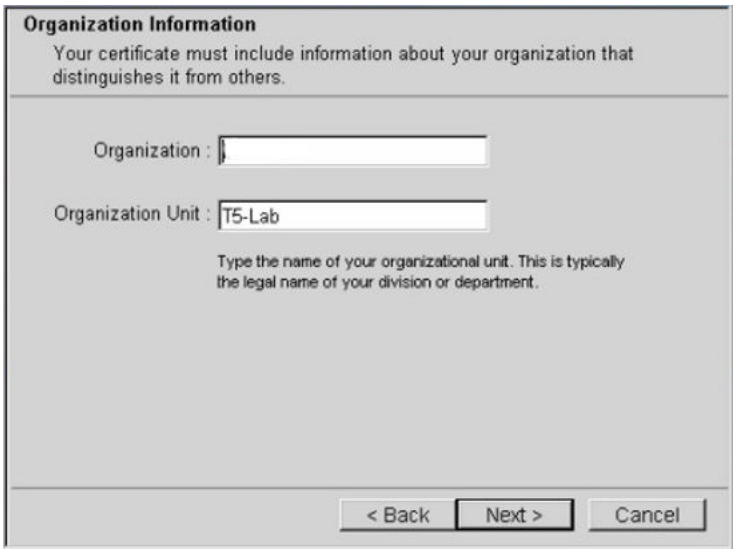
5. Select **Create a new certificate request to be signed by third party** and click **Next**.

   The Name and Security Settings window appears.



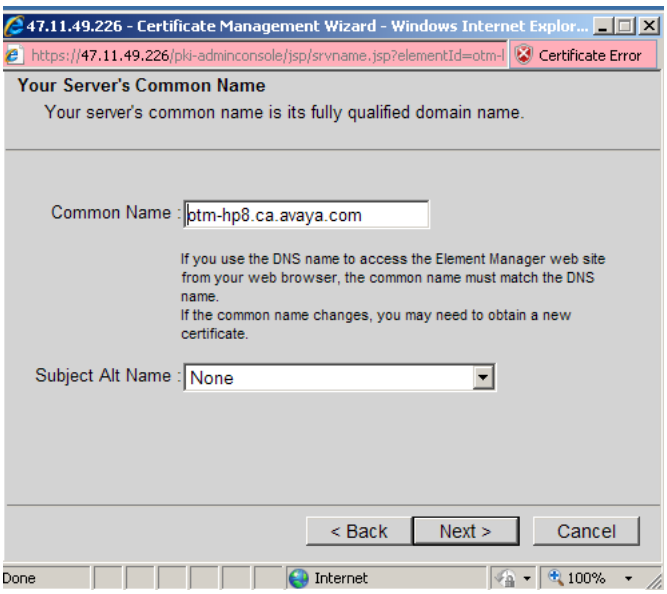
6. Type a name in the Friendly Name field.
7. Select a bit length from the **Bit length** list.
8. Click **Next**.

   The Organization Information window appears.



9. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

   The Your Server's Common Name window appears.



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

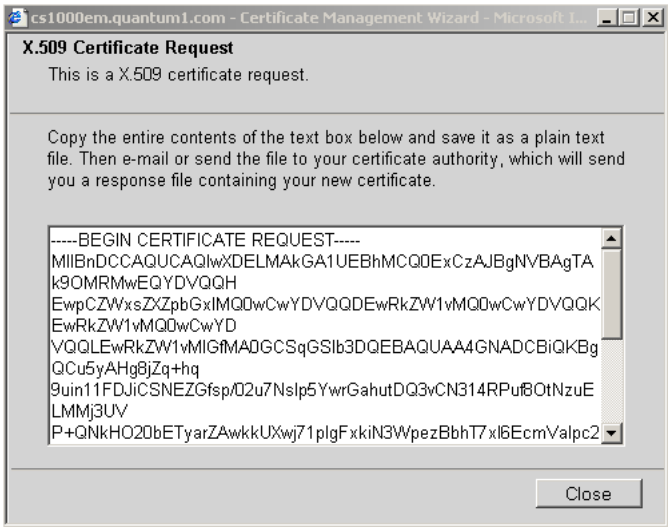
    The Geographical Information window appears.

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

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

    The Certificate Request Summary window appears.

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



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

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

    The status changes to pending.

14. Paste the certificate text into a text editor, and save it in a plain text file.
15. Send the CSR to the third-party CA.

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

    The signed certificate from the third-party CA must meet the following requirements:

    - Enhanced Key Usage (EKU): Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
    - Key Usage (KU): Digital Signature, Key Encipherment

    Key Usage extension must be marked as critical.

16. To process the pending request and install the certificate, follow the steps in Processing a pending certificate request by using UCM on page 138.

    The status changes to signed.

17. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

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

- Follow the instructions from the third-party vendor to download the intermediate CA.
- Follow the steps in Adding a CA to an endpoint on page 88 to add the intermediate CA to the browser.

Create a self-signed certificate for Web SSL

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

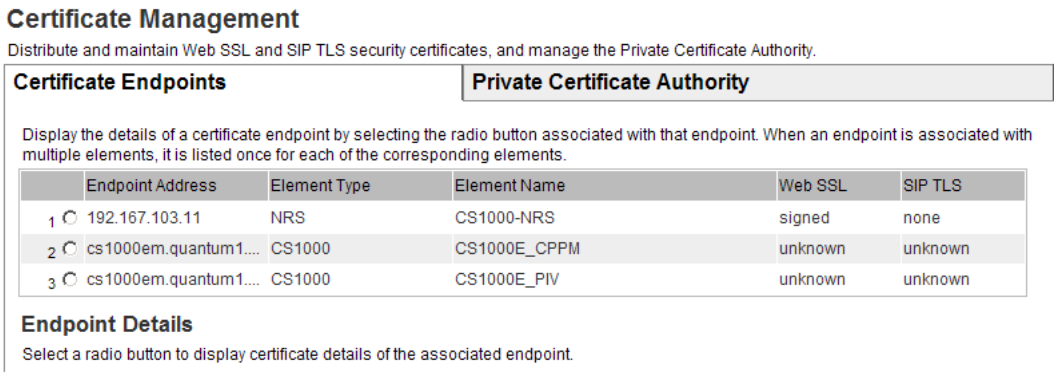
Prerequisites

- Before you create a new self-signed certificate, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a self-signed certificate for Web SSL

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

   The Certificate Management page appears.

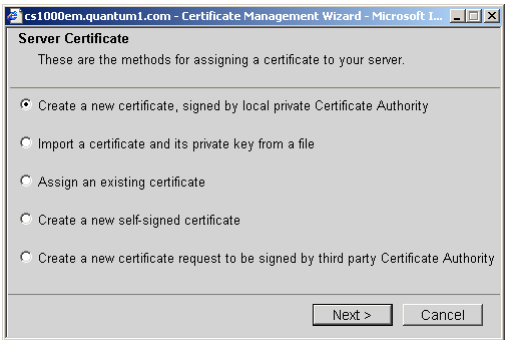


3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

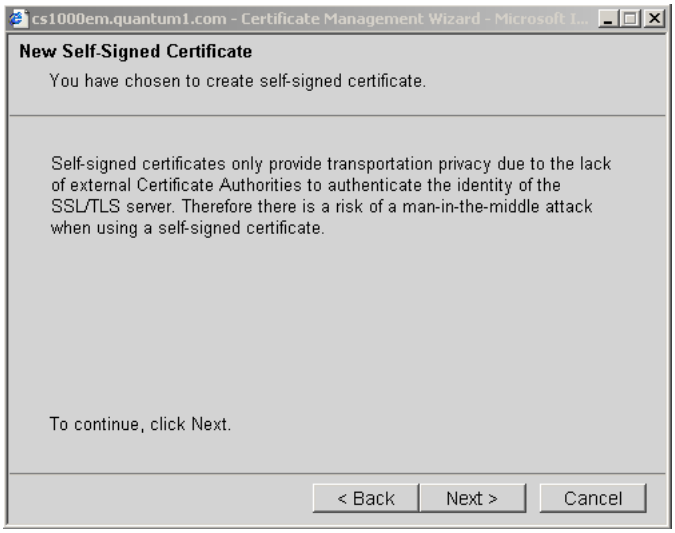
4. In the Endpoint Details pane, under Certificates, click **Web SSL**.

   The Server Certificate window appears.



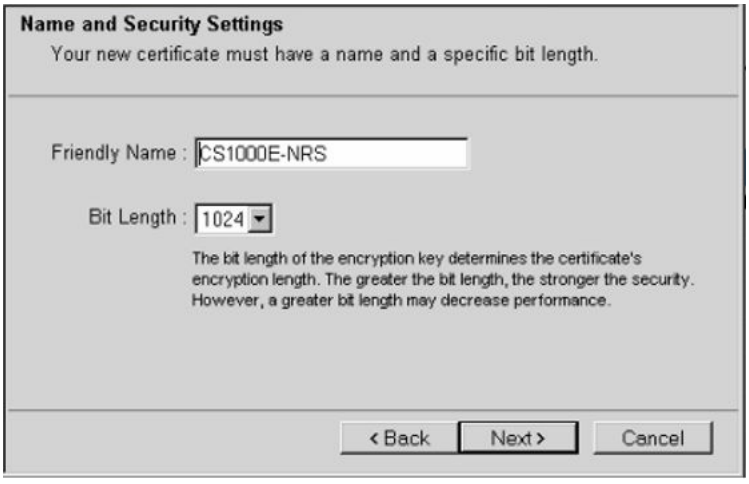
5. Select **Create a new self-signed certificate**, and click **Next**.

   The New Self-Signed Certificate window appears.



6. Click **Next**.

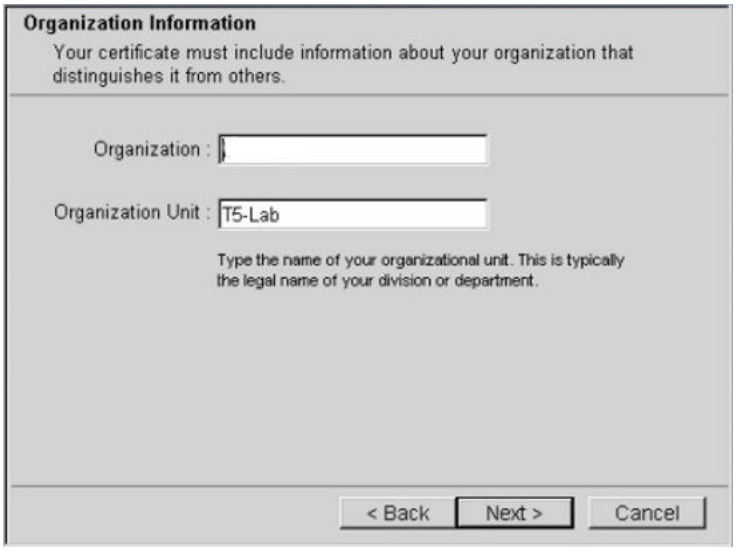
   The Name and Security Settings window appears.



7. Type a name in the Friendly Name field.
8. Select a bit length from the **Bit length** list.

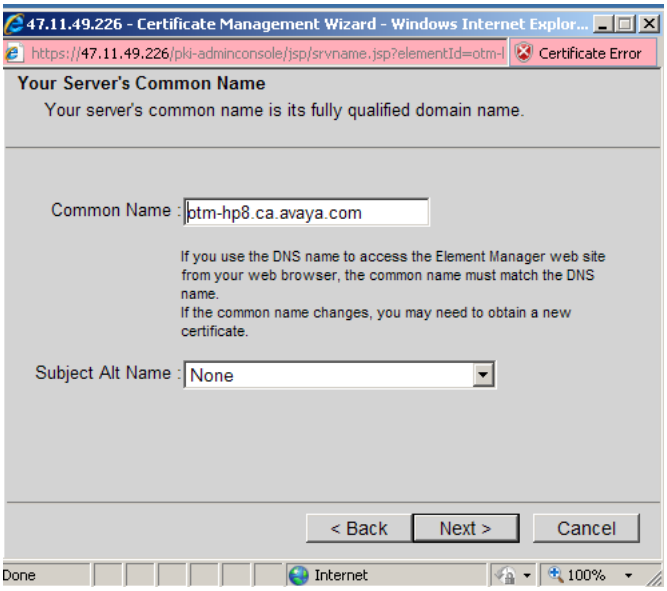
9. Click **Next**.

   The Organization Information window appears.



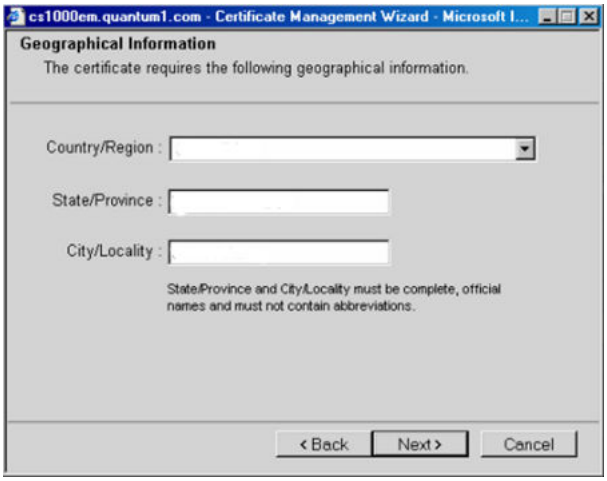
10. In the Organization Information window, perform the following tasks:
    - In the Organization field, enter the Organization.
    - In the Organization Unit field, enter the organization unit information.
    - Click Next.

    The Your Server's Common Name window appears.



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

    The Geographical Information window appears.

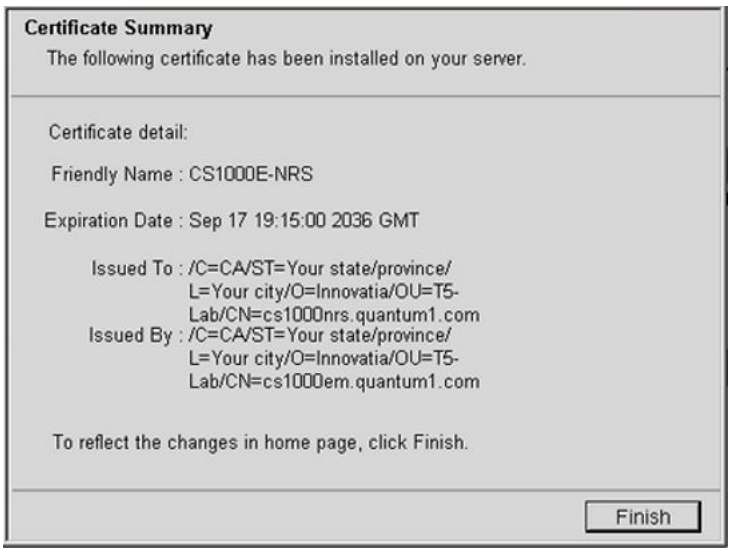


12. Enter a **Country/Region**.
13. Enter a **State/Province**.
14. Enter a **City/Locality**.
15. Click **Next**.

    The Certificate Request Summary window appears.

16. Click **Commit**.

    The **Certificate Summary** window appears.



17. Click **Finish**.

    The status changes to self-signed.

18. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

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

- Follow the steps in Exporting the current self-signed certificate by using UCM on page 144 to export the self-signed certificate.
- Follow the steps in Adding a CA to an endpoint on page 88 to add the self-signed certificate into the trusted CA list for the web browser.

Create a certificate for SIP TLS signed by the private CA

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

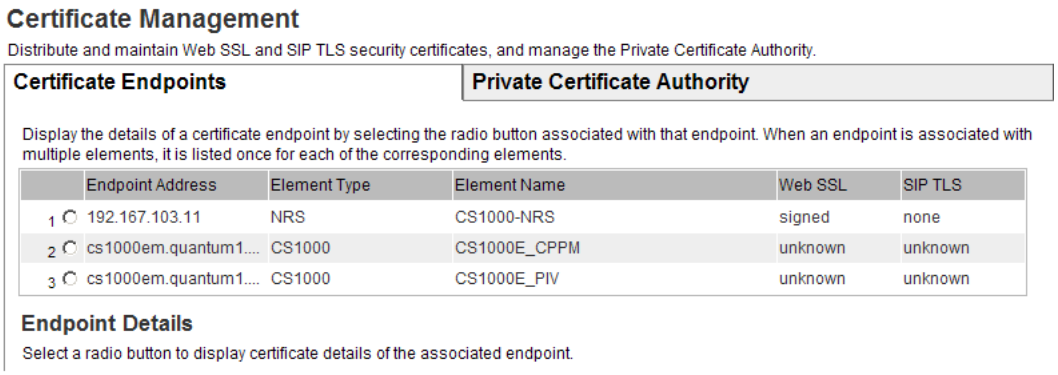
Prerequisites

- Before you create a request for a new certificate signed by a local CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a certificate for SIP TLS signed by the private CA

1. Click Security > Certificates.

   The Certificate Management page appears.

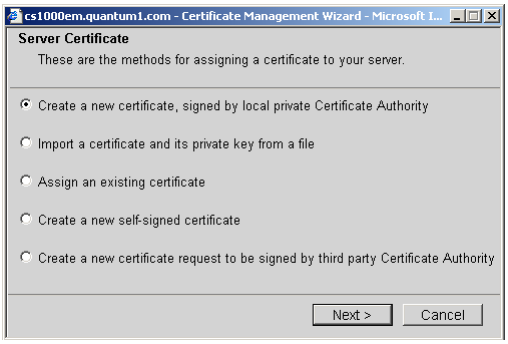


2. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

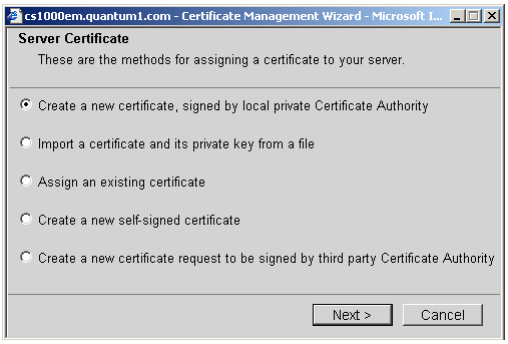
   The Endpoint Details section appears.

3. In the Endpoint Details pane, under Certificates, click **SIP TLS**.

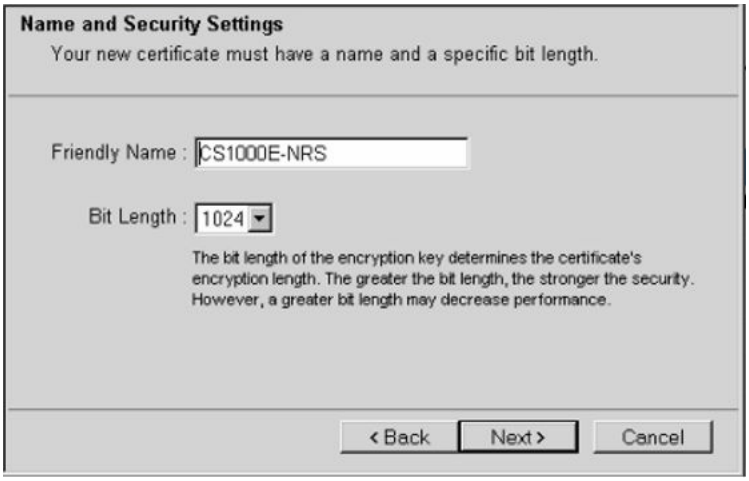
   The Server Certificate window appears.



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

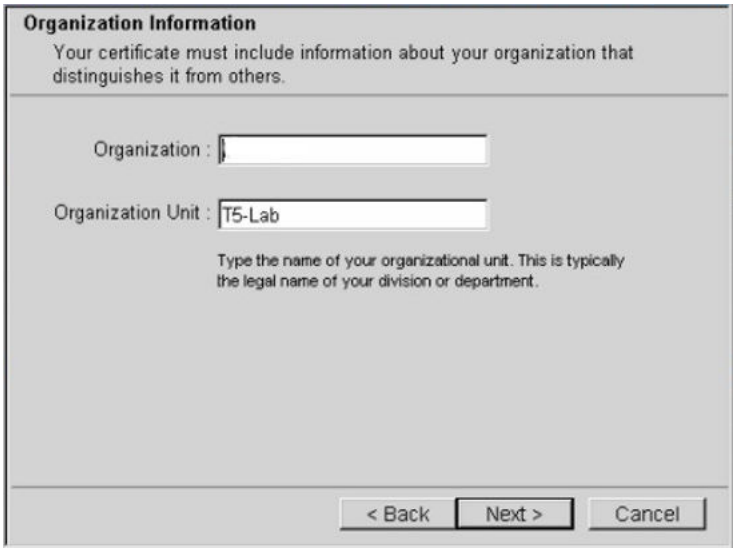


The Name and Security Settings window appears.



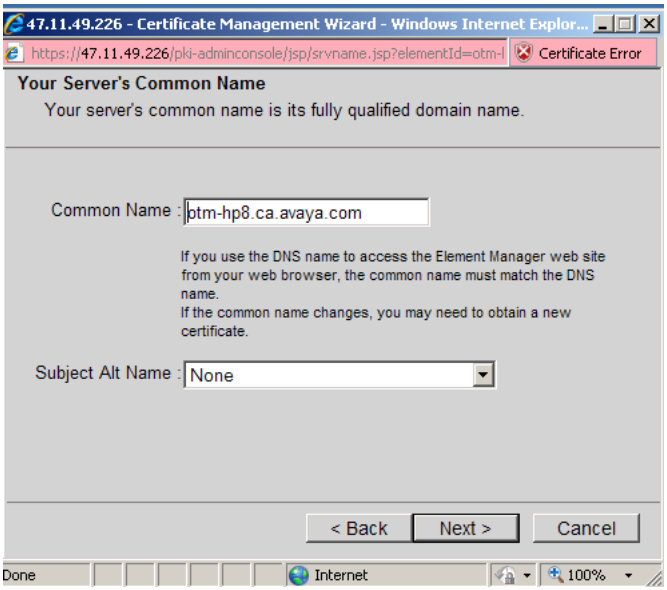
5. Type a name in the Friendly Name field.
6. Select a bit length from the **Bit length** list.
7. Click Next.

   The Organization Information window appears.



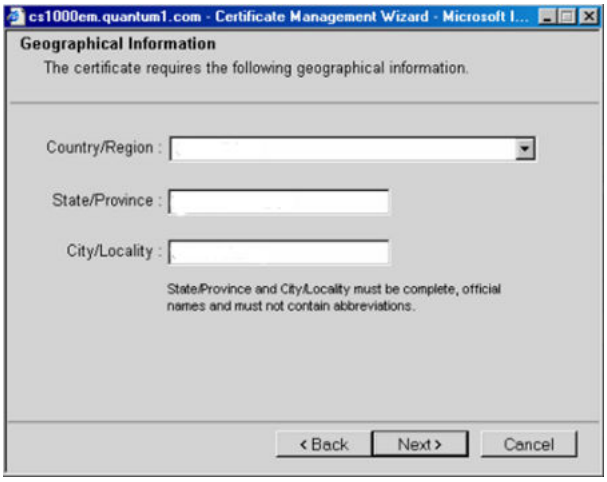
8. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

   The Your Server's Common Name window appears.



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

   The Geographical Information window appears.



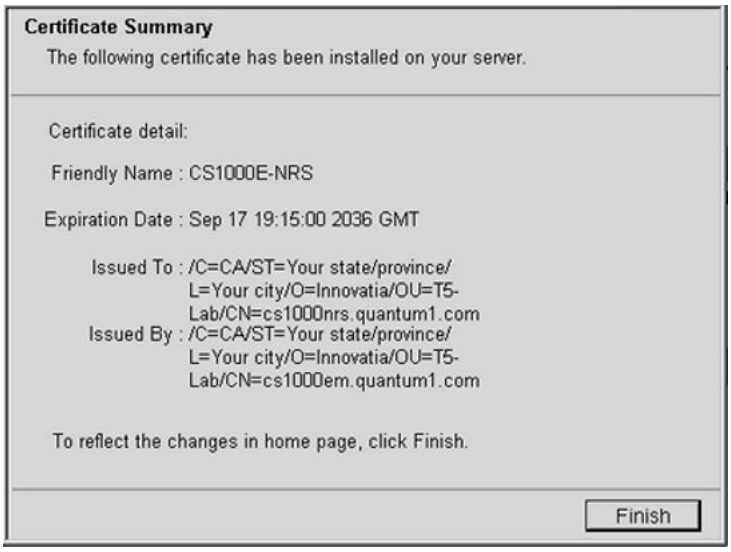
10. In the Geographical Information window, perform the following tasks:
    - In the Country/Region box, select the country from the list.
    - In the State/Province field, enter the state or province.
    - In the City/Locality field, enter the city or locality.

- Click Next.

The Certificate Request Summary window appears.

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

    A Certificate Summary window appears with the certificate information.



12. Click **Finish**.

    The status changes to signed.

13. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Create a certificate for SIP TLS signed by a public CA

Use the procedures in this section to create a certificate signed by a trusted third-party CA.

If you are upgrading a SIP Gateway system from Communication Server 1000 Release 4.5 or later, see Create a request for a third-party CA certificate for SIP TLS when upgrading the system on page 129 before you proceed.

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

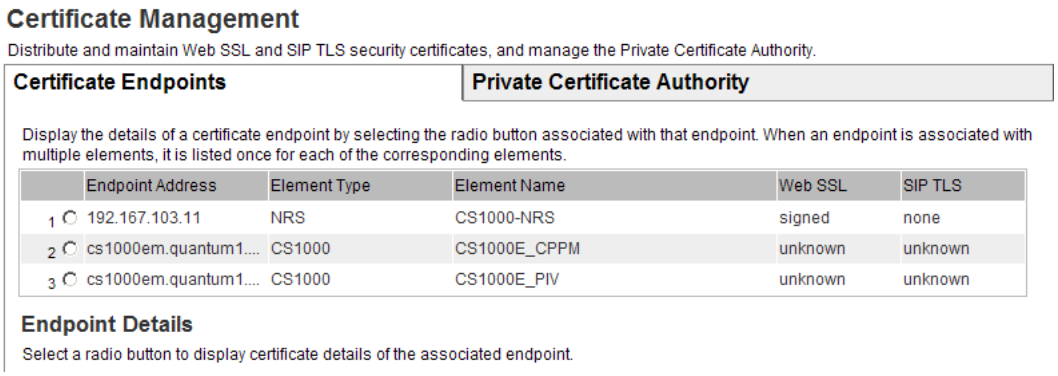
Prerequisites

- Before you create a request for a new certificate signed by a third-party CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

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

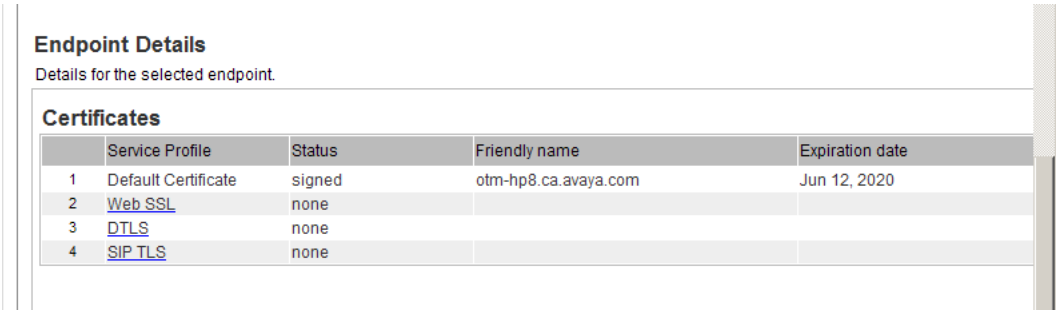
1. Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2. Click Security > Certificates.

   The Certificate Management page appears.



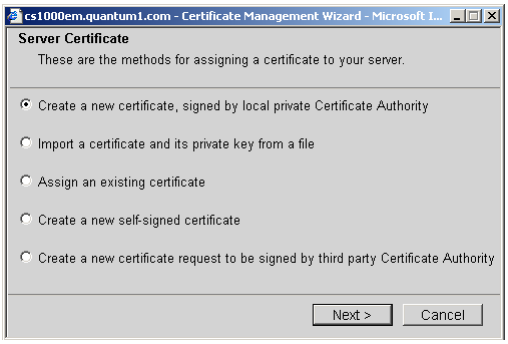
3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

   The Endpoint Details section appears.



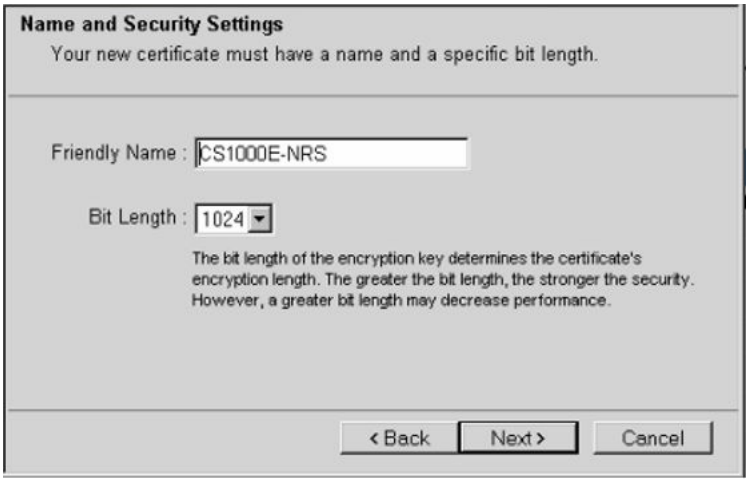
4. In the Endpoint Details pane, under Certificates, click SIP TLS.

   The Server Certificate window appears.



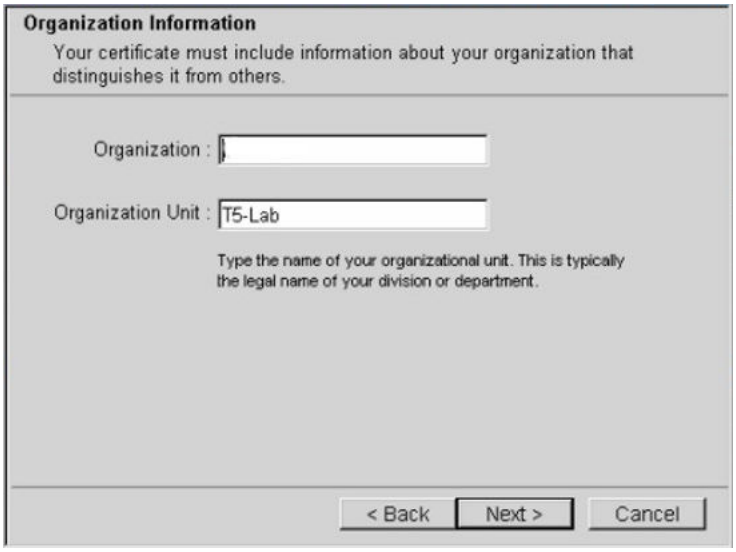
5. Select **Create a new certificate request to be signed by third party** and click **Next**.

   The Name and Security Settings window appears.



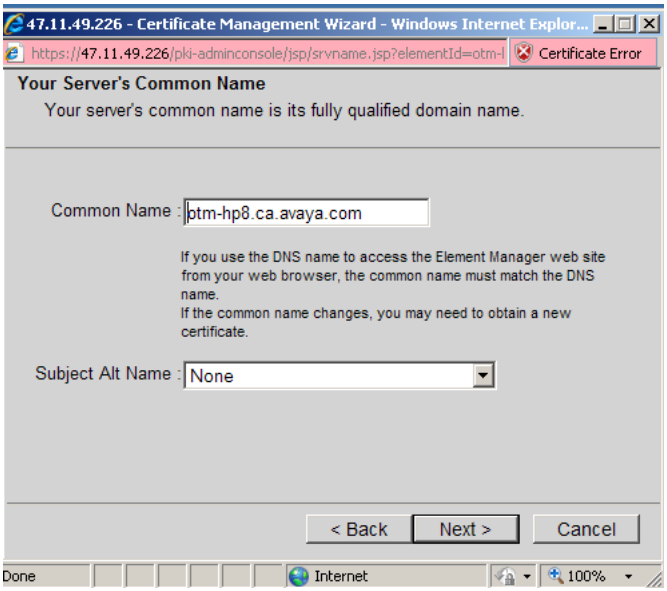
6. Type a name in the Friendly Name field.
7. Select a bit length from the **Bit length** list.
8. Click Next.

   The Organization Information window appears.



9. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

   The Your Server's Common Name window appears.



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

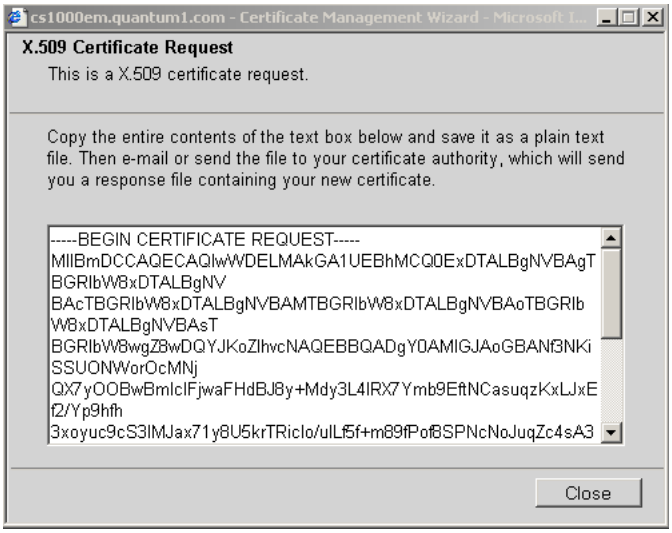
    The Geographical Information window appears.

11. In the Geographical Information window, perform the following tasks:
    - In the Country/Region box, select the country from the list.
    - In the State/Province field, enter the state or province.
    - In the City/Locality field, enter the city or locality.
    - Click Next.

    The Certificate Request Summary window appears.

12. Click Commit.

    The X.509 Certificate Request window appears.



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

13. To copy the CSR, click in the text box, press ctrl-a to select all of the text, and then press ctrl-c to copy the text.
14. Paste the certificate text into a text editor, and save it in a plain text file.
15. Click **Close**.

    The status changes to pending.

16. Send the CSR to the third-party CA.

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

17. To process the pending request and install the certificate, follow the steps in Processing a pending certificate request by using UCM on page 138.

    The status changes to signed.

18. Follow the instructions from the third-party CA to download the certificates for the intermediate and root CAs.
19. Follow the steps in Adding a CA to an endpoint on page 88 to add the intermediate CA to the server.

    For more information about certificate chains, see Table 4: Examples of certificates in a chain on page 27.
20. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Create a certificate for DTLS signed by the private CA

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

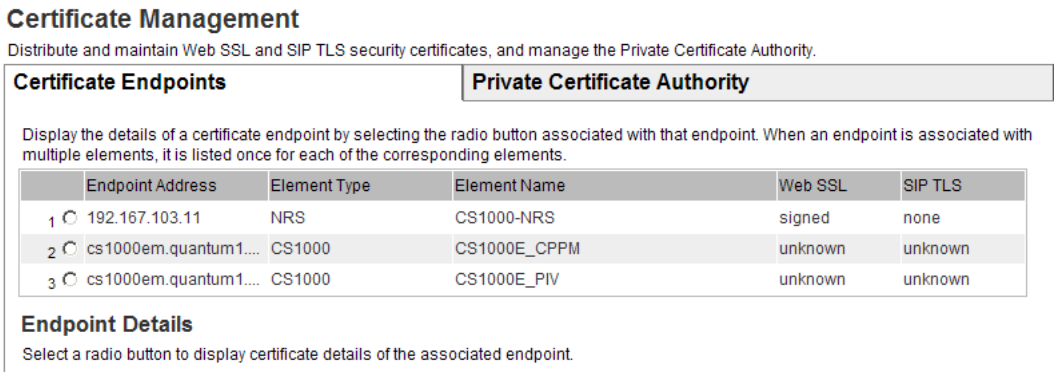
Prerequisites

- Before you create a request for a new certificate signed by a local CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a certificate for DTLS signed by the private CA

1. Click Security > Certificates.

   The Certificate Management page appears.

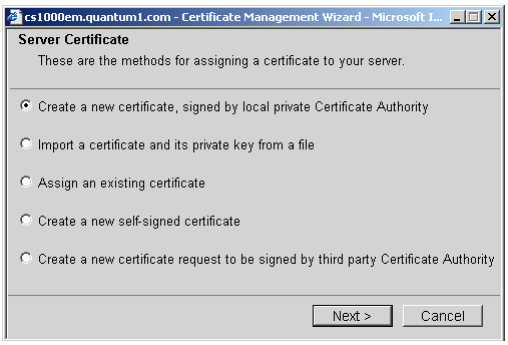


2. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

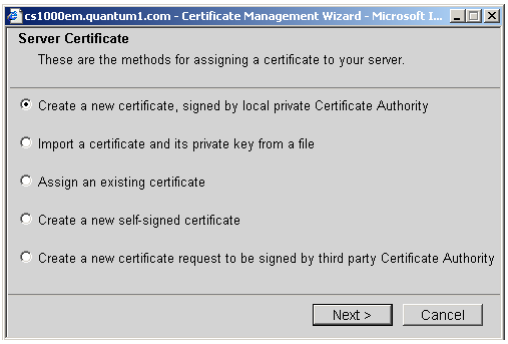
   The Endpoint Details section appears.

3. In the Endpoint Details pane, under Certificates, click **DTLS**.

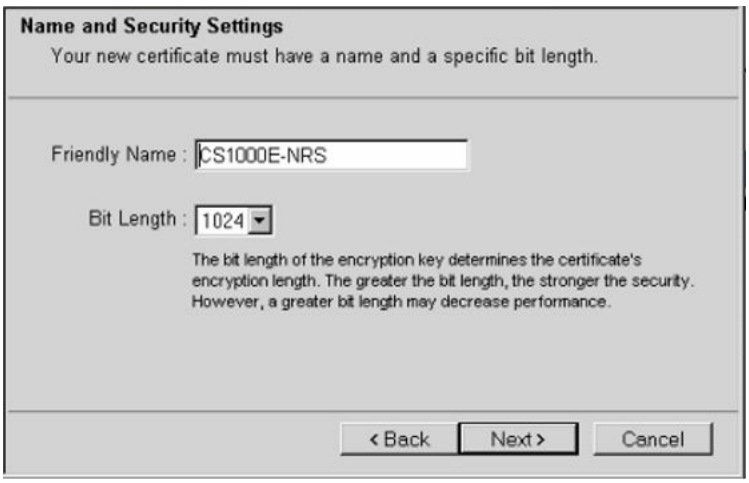
   The Server Certificate window appears.



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

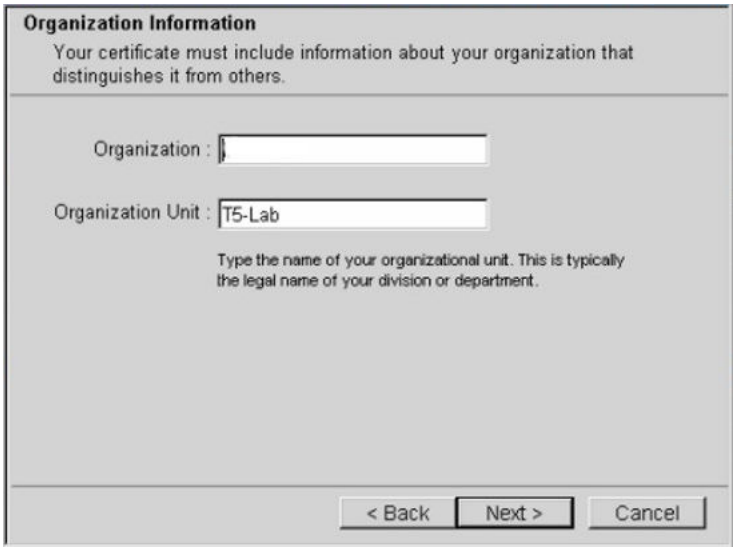


   The Name and Security Settings window appears.



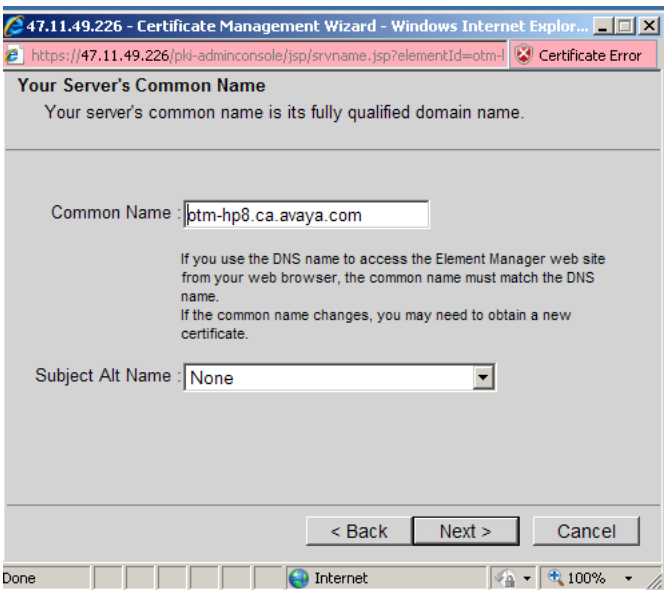
5. Type a name in the Friendly Name field.
6. Select a bit length from the **Bit length** list.
7. Click Next.

   The Organization Information window appears.



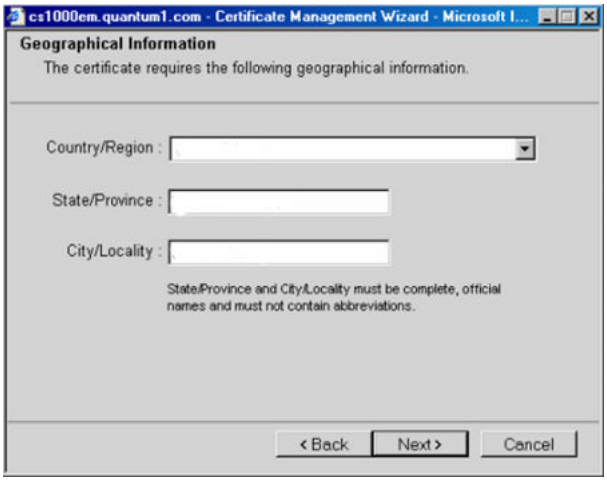
8. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

   The Your Server's Common Name window appears.



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

   The Geographical Information window appears.

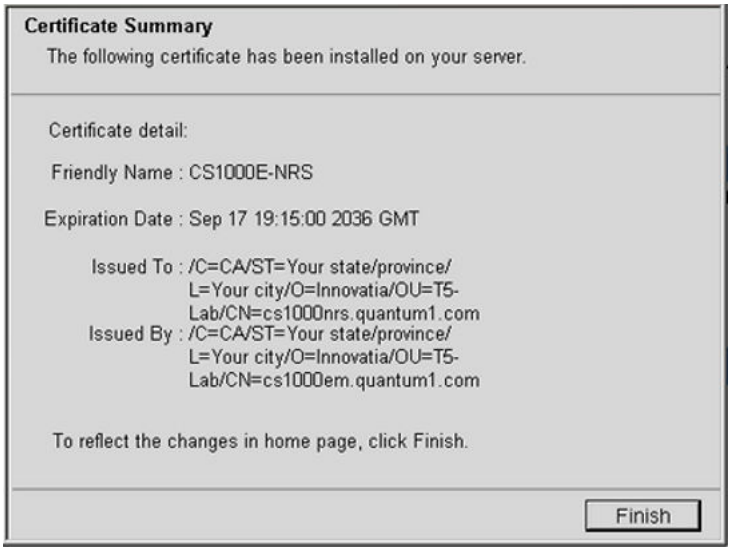


10. In the Geographical Information window, perform the following tasks:
    - In the Country/Region box, select the country from the list.
    - In the State/Province field, enter the state or province.
    - In the City/Locality field, enter the city or locality.
    - Click Next.

    The Certificate Request Summary window appears.

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

    A Certificate Summary window appears with the certificate information.



12. Click **Finish**.

    The status changes to signed.

13. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Create a certificate for DTLS signed by a public CA

Use the procedures in this section to create a certificate signed by a trusted third-party CA.

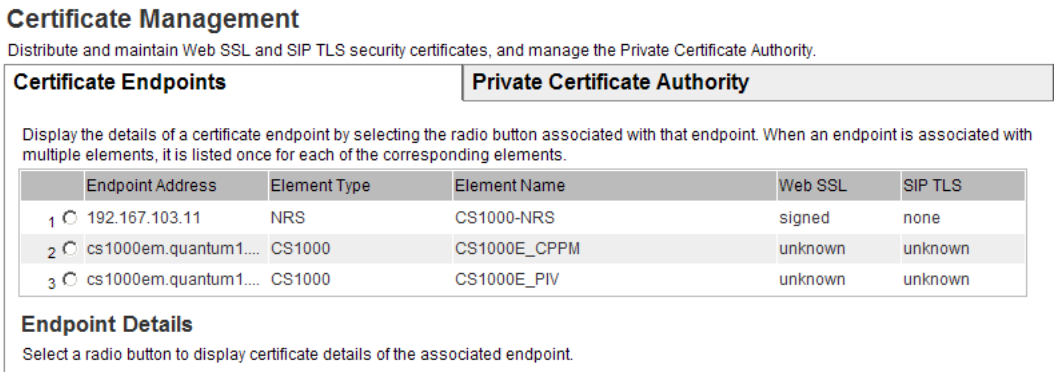
Prerequisites

- Before you create a request for a new certificate signed by a third-party CA, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a request for a certificate for DTLS signed by a public CA

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

   The Certificate Management page appears.

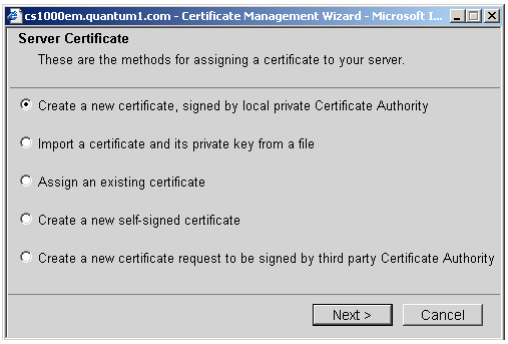


3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure; the certificate endpoint status must be none.

   The Endpoint Details section appears.

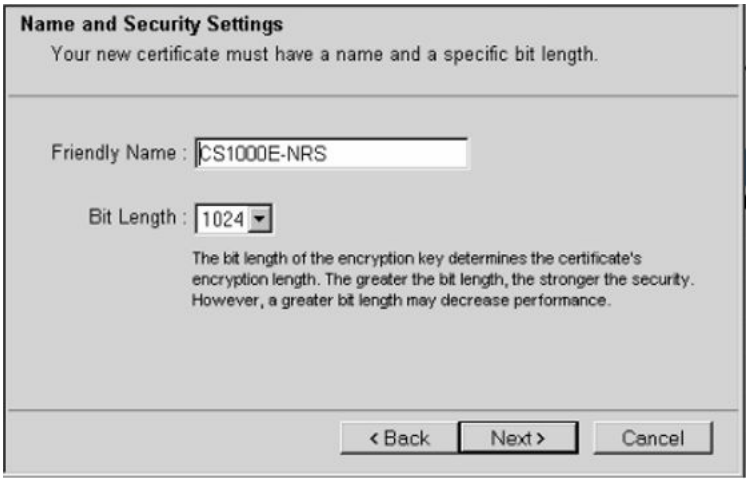
4. In the Endpoint Details pane, under Certificates, click DTLS.

   The Server Certificate window appears.



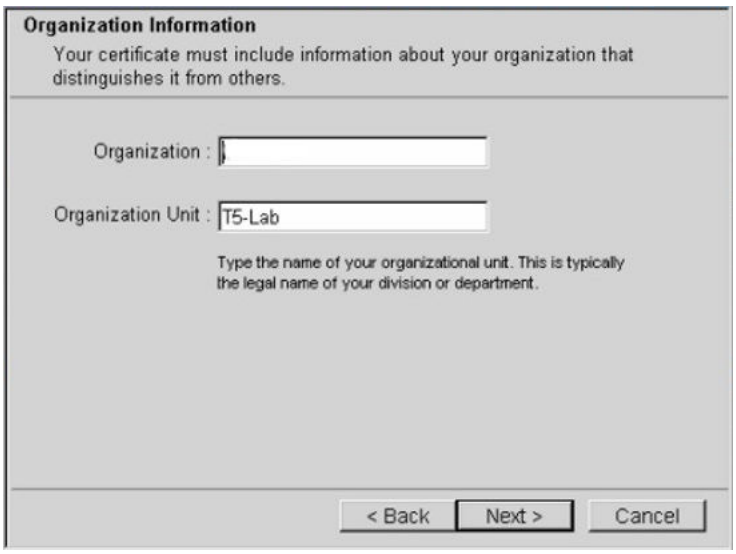
5. Select **Create a new certificate request to be signed by third party** and click **Next**.

   The Name and Security Settings window appears.



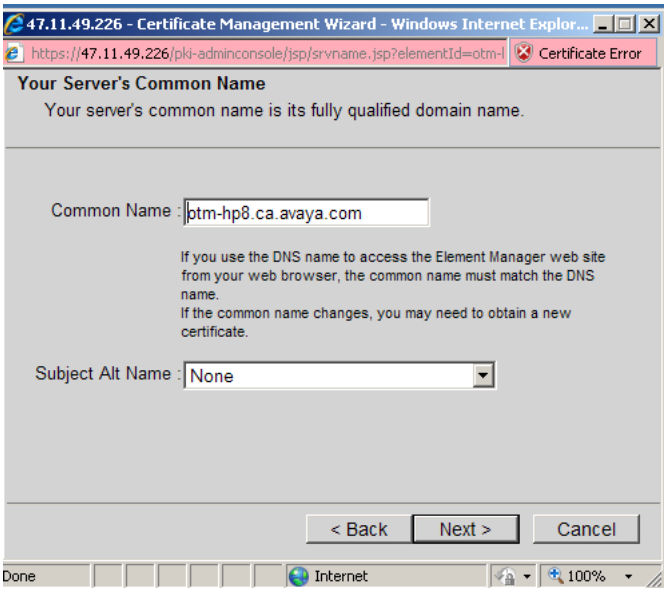
6. Type a name in the Friendly Name field.
7. Select a bit length from the **Bit length** list.
8. Click Next.

   The Organization Information window appears.



9. In the Organization Information window, perform the following tasks:
   - In the Organization field, enter the Organization.
   - In the Organization Unit field, enter the organization unit information.
   - Click Next.

   The Your Server's Common Name window appears.



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

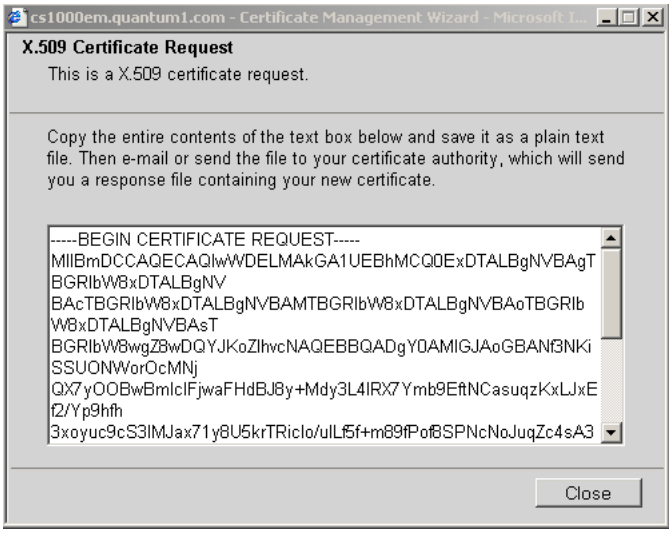
    The Geographical Information window appears.

11. In the Geographical Information window, perform the following tasks:
    - In the Country/Region box, select the country from the list.
    - In the State/Province field, enter the state or province.
    - In the City/Locality field, enter the city or locality.
    - Click Next.

    The Certificate Request Summary window appears.

12. Click Commit.

    The X.509 Certificate Request window appears.



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

13. To copy the CSR, click in the text box, press ctrl-a to select all of the text, and then press ctrl-c to copy the text.
14. Paste the certificate text into a text editor, and save it in a plain text file.
15. Click **Close**.

    The status changes to pending.

16. Send the CSR to the third-party CA.

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

17. To process the pending request and install the certificate, follow the steps in Processing a pending certificate request by using UCM on page 138.

    The status changes to signed.

18. Follow the instructions from the third-party CA to download the certificates for the intermediate and root CAs.
19. Follow the steps in Adding a CA to an endpoint on page 88 to add the intermediate CA to the server.

    For more information about certificate chains, see Table 4: Examples of certificates in a chain on page 27.
20. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Create a request for a third-party CA certificate for SIP TLS when upgrading the system

When you upgrade a SIP Gateway System from Communication Server 1000 Release 4.5, the steps to install third-party CA-signed certificates vary depending on whether you request and install the certificate before upgrading, or after upgrading.

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

If you have already upgraded the system from Communication Server 1000 Release 4.5 or later, see Creating a request for a certificate for SIP TLS signed by a public CA on page 116. If you have not yet upgraded the system see Creating a request for a certificate signed by a third-party CA for SIP TLS when upgrading on page 129 before you perform the system upgrade.

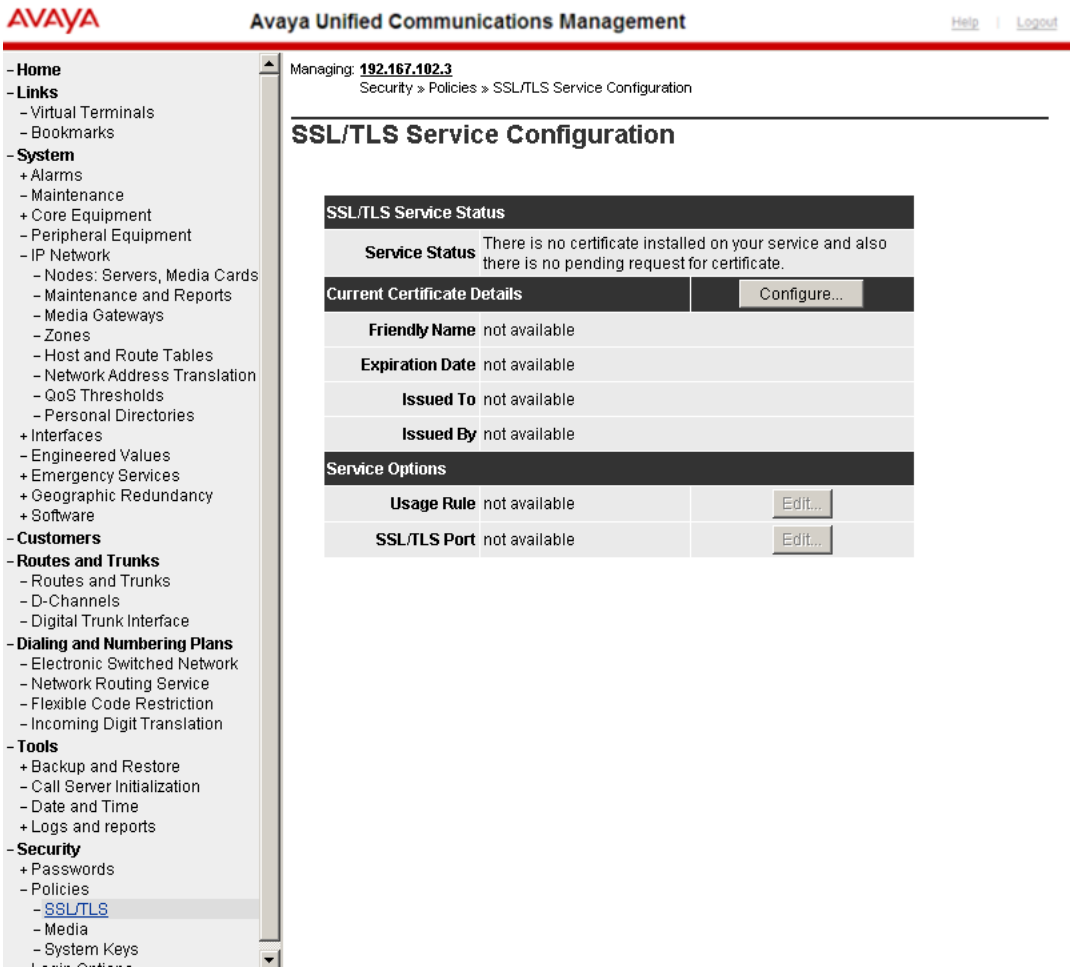
Prerequisites

- 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.

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

1. Before upgrading from CS 1000 Release 5.5, log on to Element Manager using a System password level 2 account.
2. Click **Security > Policies > SSL/TLS**.

   The SSL/TLS Service Configuration page appears.



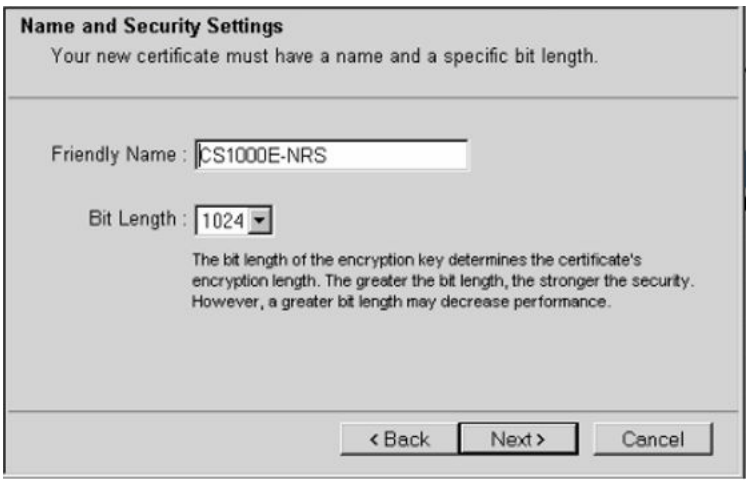
3. Click **Configure**.

   The Server Certificate window appears.

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

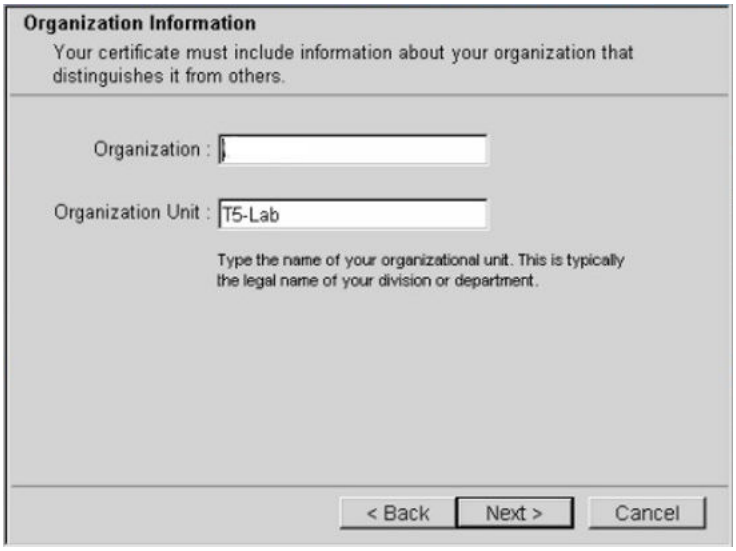
5. Click **Next**.

   The Name and Security Settings window appears.



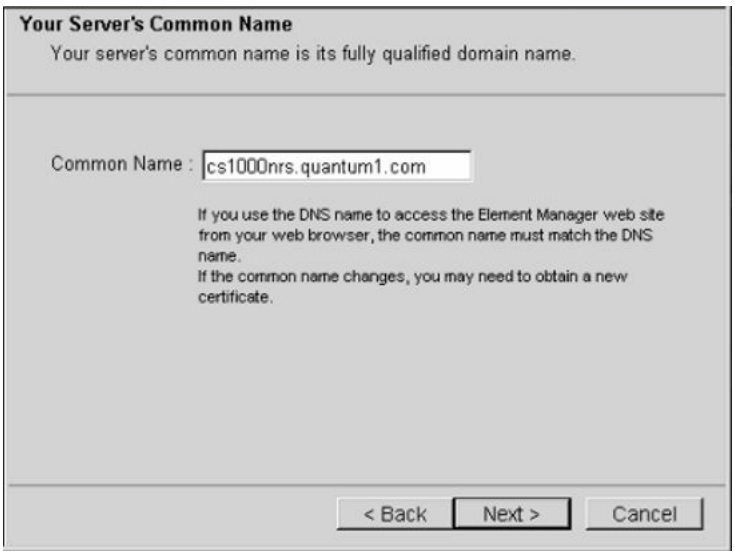
6. Type a name in the **Friendly Name** field.
7. Select a bit length from the **Bit length** list.
8. Click **Next**.

   The Organization Information window appears.



9. In the **Organization Information** window, perform the following tasks:
   - In the **Organization** field, enter the Organization.
   - In the **Organization Unit** field, enter the organization unit information.
   - Click **Next**.

   The Your Server's Common Name window appears.



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

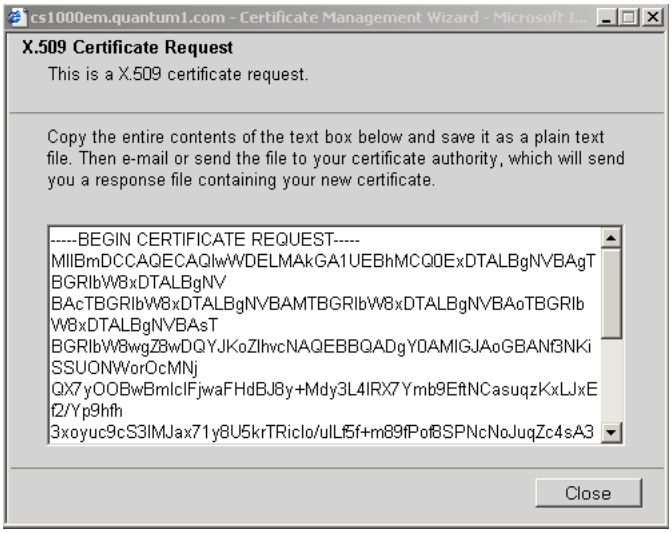
    The Geographical Information window appears.

11. Perform the following tasks:

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

    The Certificate Request Summary window appears.

12. The X.509 Certificate Request window appears.



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

13. To copy the CSR, click in the text box, press `ctrl-a` to select all of the text, and then press `ctrl-c` to copy the text.
14. Paste the certificate text into a text editor, and save it in a plain text file.
15. Click **Close**.

    The status changes to: There is a pending new Certificate request on your service.
16. Send the CSR to the third-party CA.

Use the following procedure to process a pending certificate response using Element Manager. If you have already upgraded the system from Communication Server 1000 Release 5.x to Communication Server 1000 Release 7.x, see Creating a request for a certificate for SIP TLS signed by a public CA on page 116

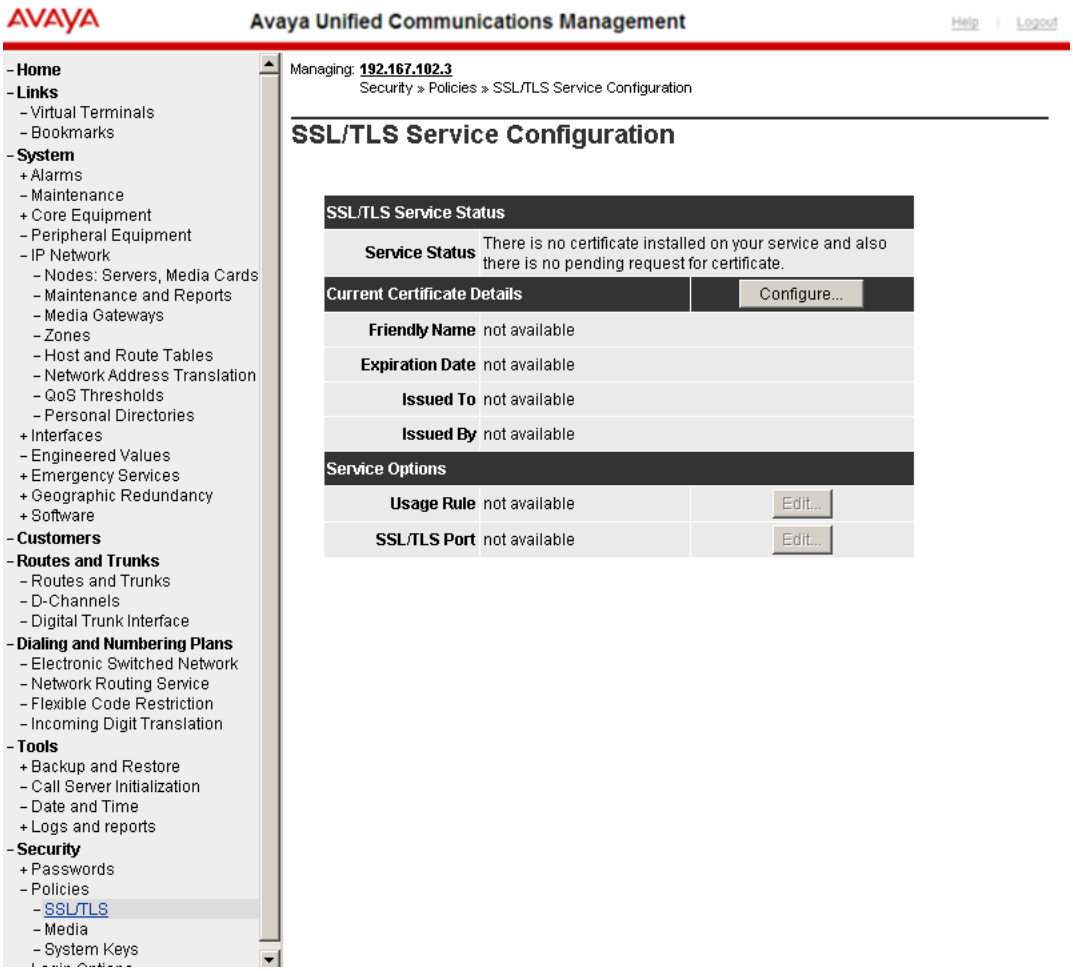
Prerequisites

- 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.

Processing a pending certificate response for SIP TLS when upgrading

1. Before upgrading from CS 1000 Release 5.x, log on to Element Manager using a System password level 2 account.
2. Click **Security > Policies > SSL/TLS**.

   The SSL/TLS Service Configuration page appears.



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 7.x.
8. Follow the steps inAssigning an existing certificate by using UCM on page 150 to assign the installed third-party CA certificate.
9. Use the steps in Adding a CA to an endpoint on page 88 to add the certificate to the trusted CA list on each of the endpoints that must communicate with the element that owns this certificate.
10. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Create a self-signed certificate for SIP TLS

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

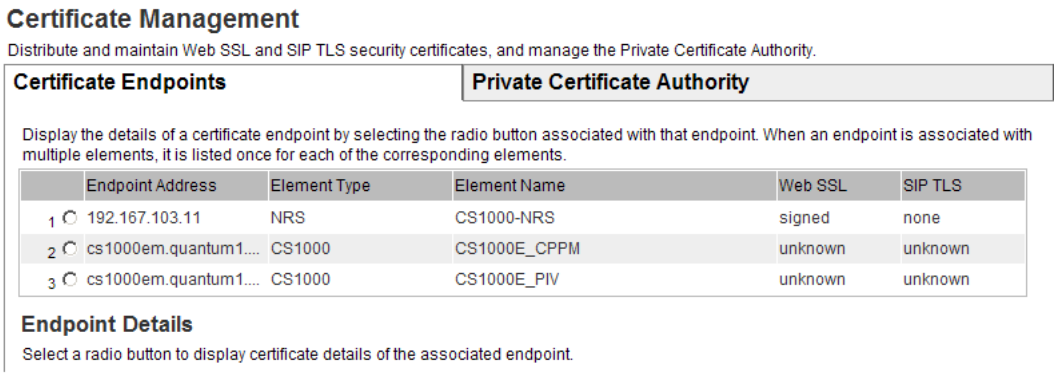
Prerequisites

- Before you create a new self-signed certificate, ensure that the certificate endpoint status is none. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Creating a self-signed certificate for SIP TLS

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

   The Certificate Management page appears.

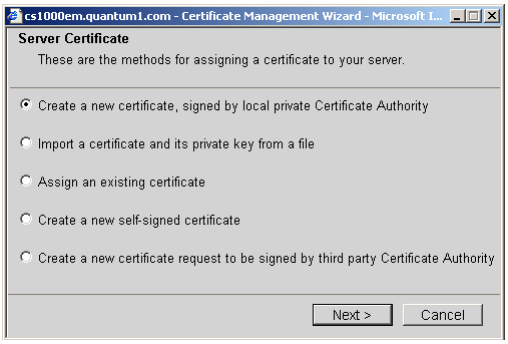


3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

4. In the Endpoint Details pane, under Certificates, click SIP TLS.

   The Server Certificate window appears.

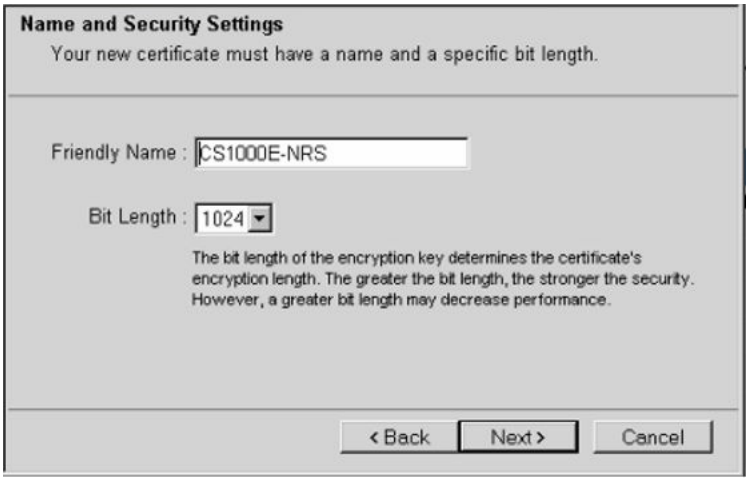


5. Select **Create a new self-signed certificate**, and click **Next**.

   The New Self-Signed Certificate window appears.

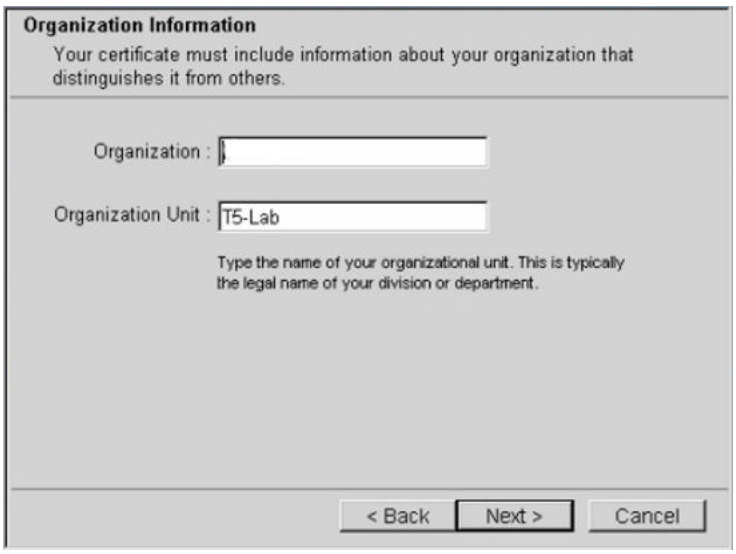
6. Click **Next**.

   The Name and Security Settings window appears.



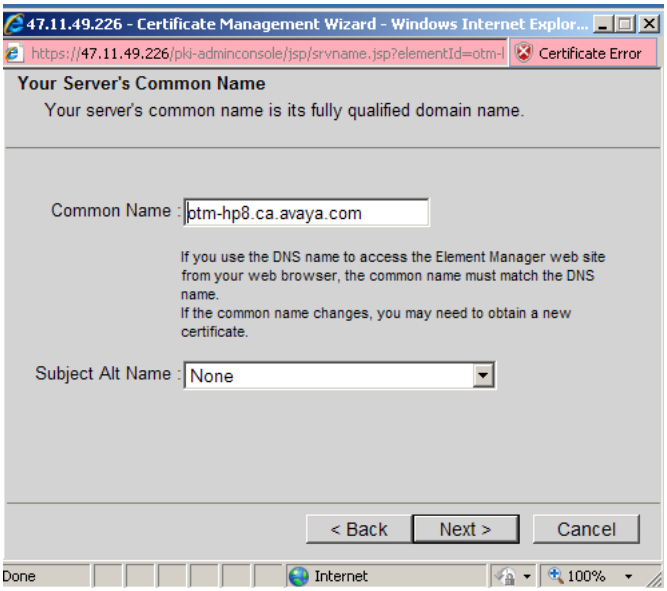
7. Type a name in the Friendly Name field.
8. Select a bit length from the **Bit length** list.
9. Click **Next**.

   The Organization Information window appears.



10. In the Organization Information window, perform the following tasks:
    - In the Organization field, enter the Organization.
    - In the Organization Unit field, enter the organization unit information.
    - Click Next.

    The Your Server's Common Name window appears.



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

    The Geographical Information window appears.
12. Enter a **Country/Region**.
13. Enter a **State/Province**.
14. Enter a **City/Locality**.

15. Click **Next**.

    The Certificate Request Summary window appears.
16. Click **Commit**.

    The **Certificate Summary** window appears.
17. Click **Finish**.

    The status changes to self-signed.
18. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.
19. Use the steps in Exporting the current self-signed certificate by using UCM on page 144 to export the self-signed certificate.
20. Use the steps in Adding a CA to an endpoint on page 88 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.

Process a pending certificate response

To create a request for a CA to sign a certificate, see Create a certificate for SIP TLS signed by a public CA on page 115. 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.

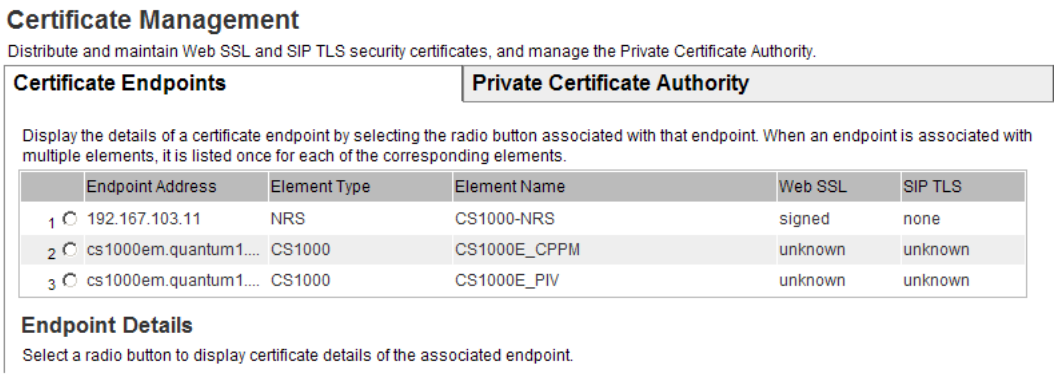
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Processing a pending certificate request by using UCM

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

   The Certificate Management page appears.

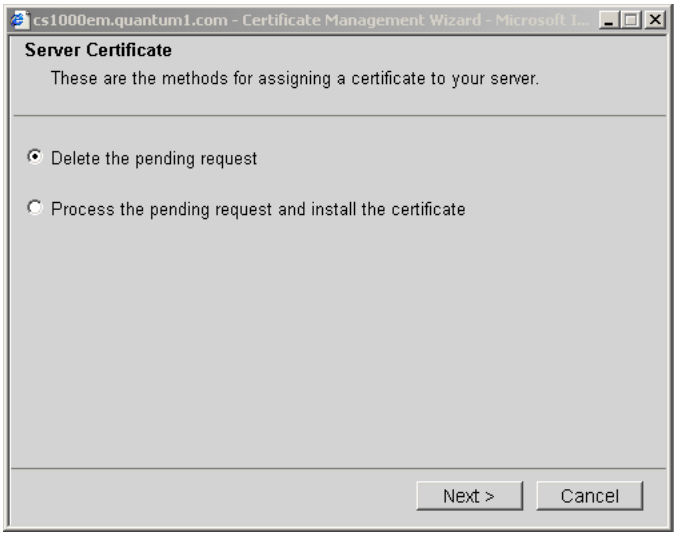


3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

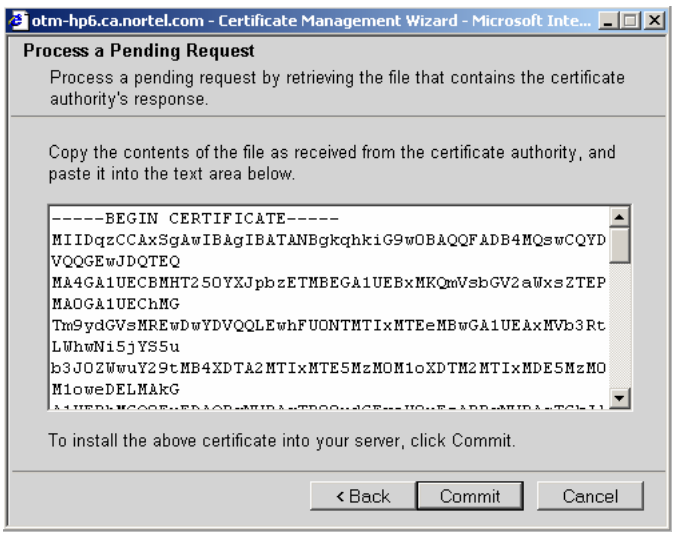
4. In the Endpoint Details pane, under Certificates, click SIP TLS or **Web SSL**.

   The Server Certificate window appears.



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

   The Process a Pending Request window appears.



6. Copy the contents of the text file you received from the CA and paste it in the text area.
7. Click **Commit**.

   The Certificate Summary window appears.
8. Click **Finish**.

   The service status changes to signed.

Delete a pending certificate request

Use the following procedure to delete a pending certificate request.

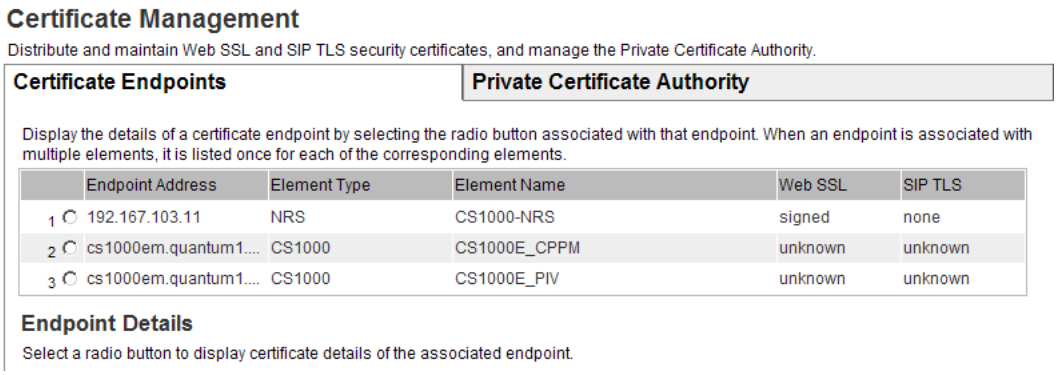
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Deleting a pending certificate request by using UCM

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

   The Certificate Management page appears.



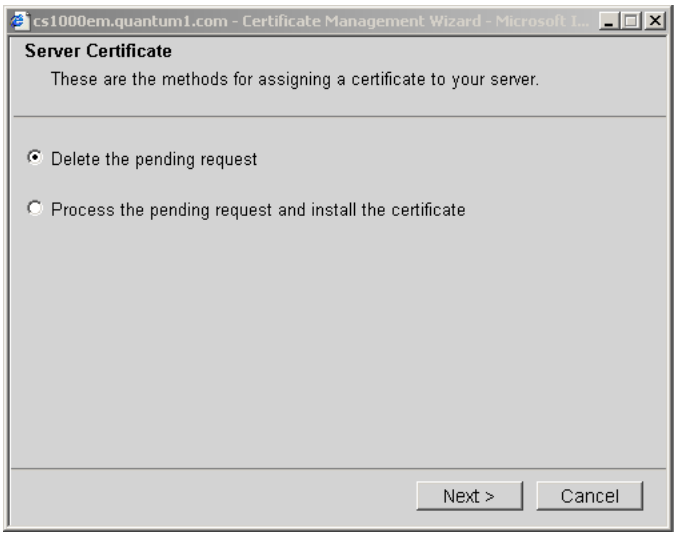
3. In the Certificate Endpoints pane, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

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

   The Server Certificate window appears.

   The Server Certificate window appears.



5. Select **Delete the pending request**, and click **Next**.

   The Delete a Pending Request window appears.

6. Click **Finish**.

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.

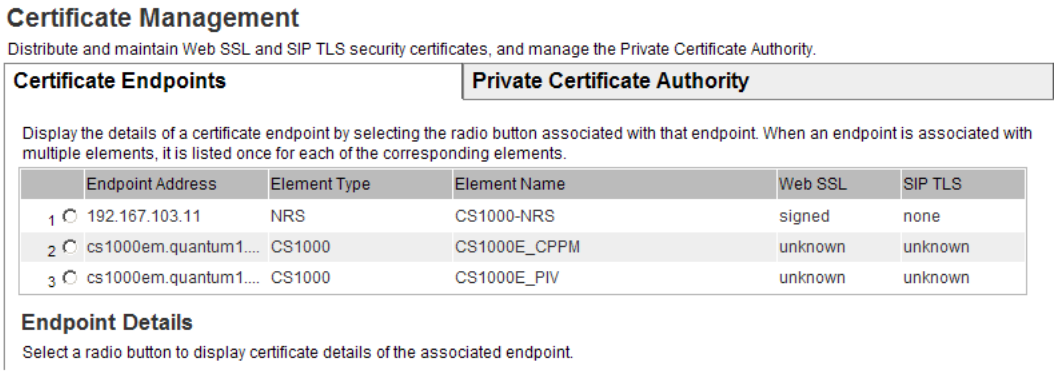
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Creating a certificate renew request by using UCM

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

   The Certificate Management page appears.

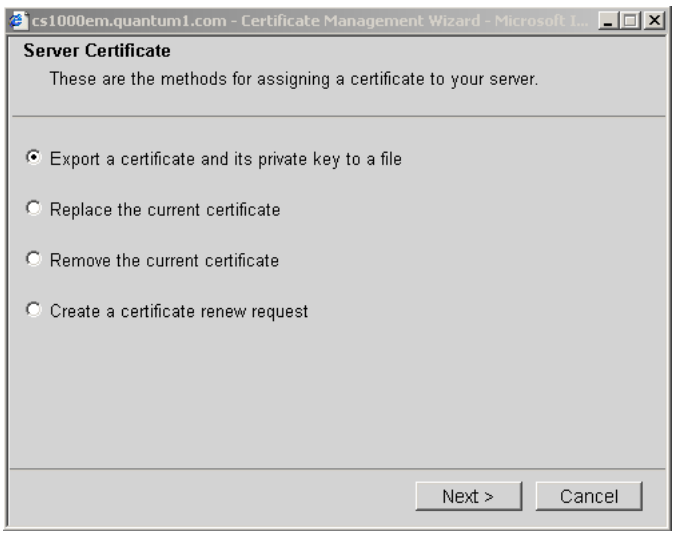


3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

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

   The Server Certificate window appears.

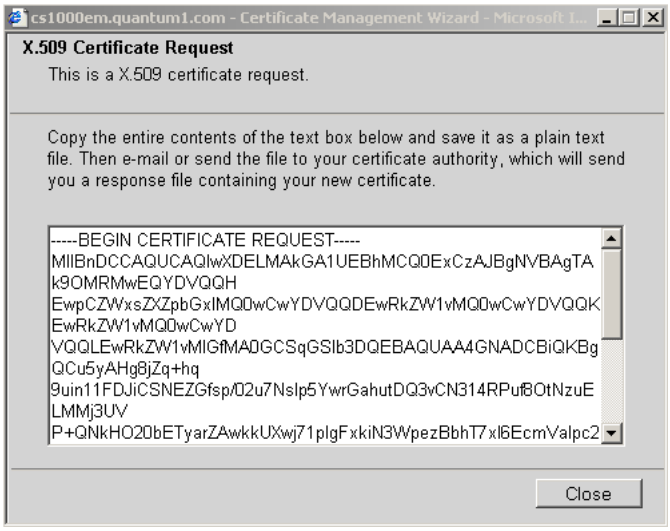


5. Select **Create a certificate renew request**, and click **Next**.

   The Renew Certificate window appears.

6. Click **Commit** to download the certificate request to a local file.

   The X.509 Certificate Request window appears. The X.509 Certificate Request window contains the CSR.



7. To copy the CSR, click in the text box, press ctrl-a to select all of the text, and then press ctrl-c to copy the text.
8. Paste the certificate text into a text editor, and save it in a plain text file.
9. Click **Close**.

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.

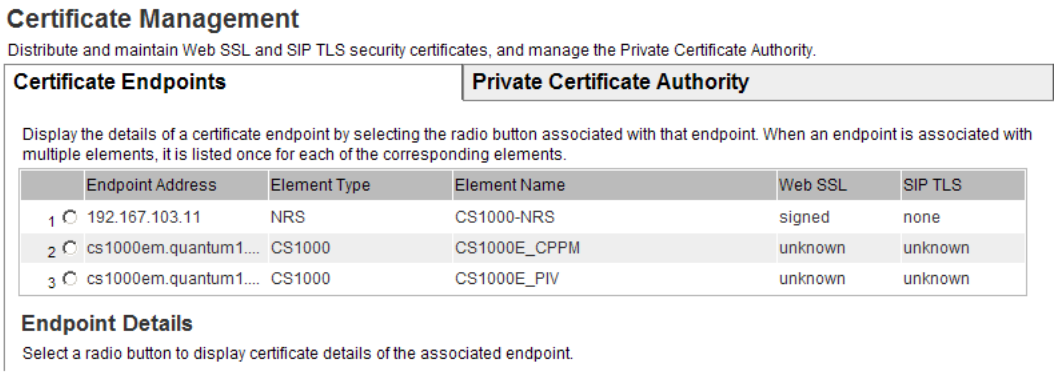
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Exporting the current self-signed certificate by using UCM

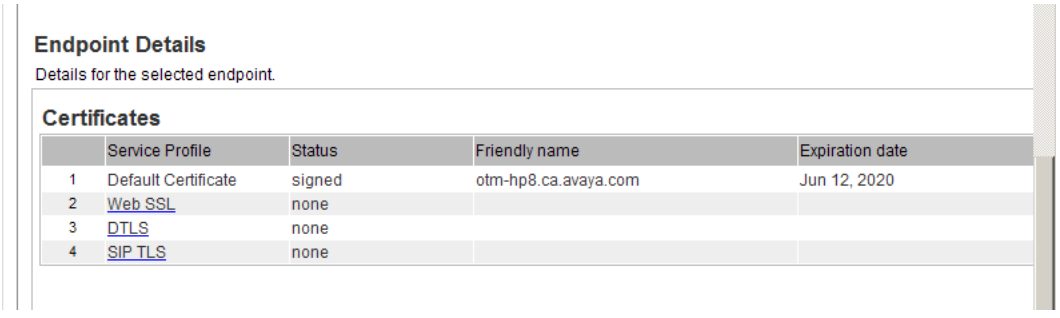
1. Log on to the UCM primary security server using an account that has SecurityAdministrator privilege.
2. Click Security > Certificates.

   The Certificate Management page appears.



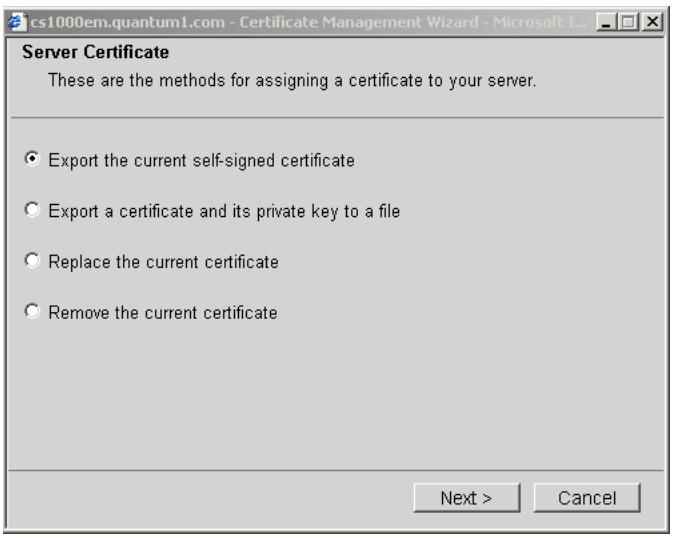
3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.



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

   The Server Certificate window appears.



5. Select **Export the current self-signed certificate**, and click **Next**.

   The Export Certificate Content window appears.
6. To copy the certificate information, click in the text box, press ctrl-a to select all of the text, and then press ctrl-c to copy the text.
7. Paste the certificate text into a text editor, and save it in a plain text file.
8. Click **Close**.

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 on page 147.

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

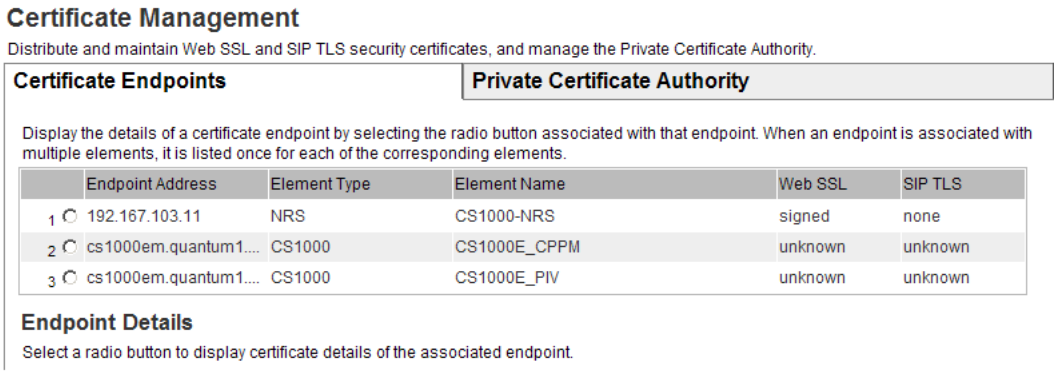
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Exporting the current certificate and its private key by using UCM

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

The Certificate Management page appears.



3. In the Certificate Endpoints tab, select the radio button next to the endpoint from which you want to export the certificate and key.

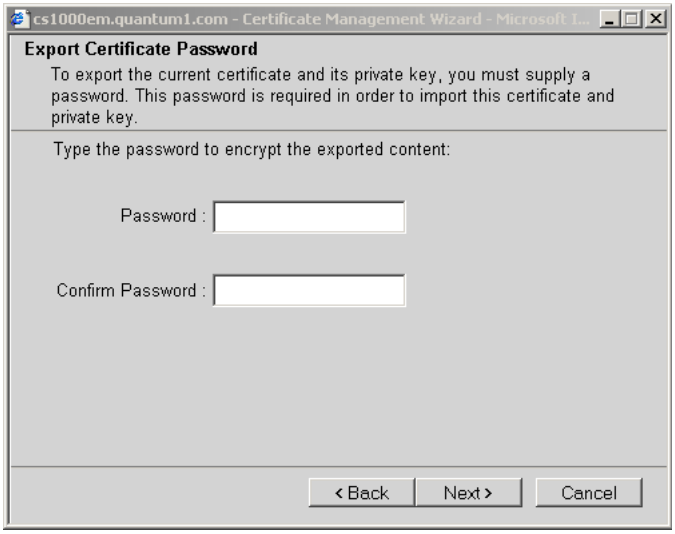
   The Endpoint Details section appears.

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

   The Server Certificate window appears.

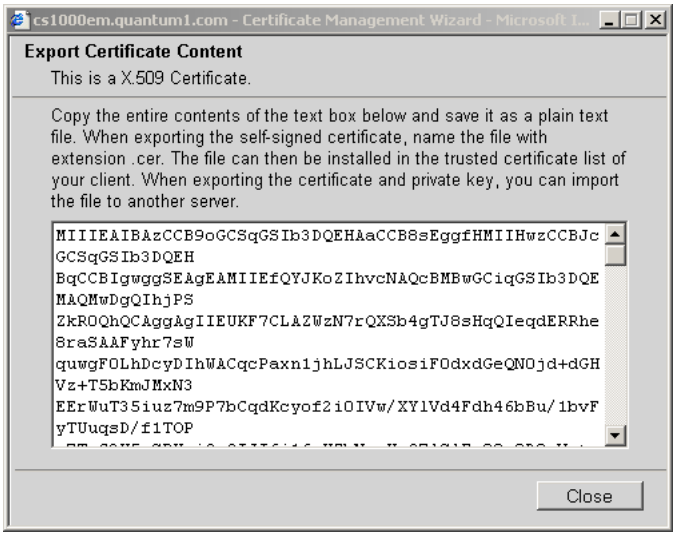
5. Select **Export a certificate and its private key to a file**, and click **Next**.

   The Export Certificate Password window appears.



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

   The Export Certificate Content window appears.



7. To copy the certificate information, click in the text box, press ctrl-a to select all of the text, and then press ctrl-c to copy the text.
8. Paste the certificate text into a text editor, and save it in a plain text file.
9. Click **Close**.

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 on page 145. 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.

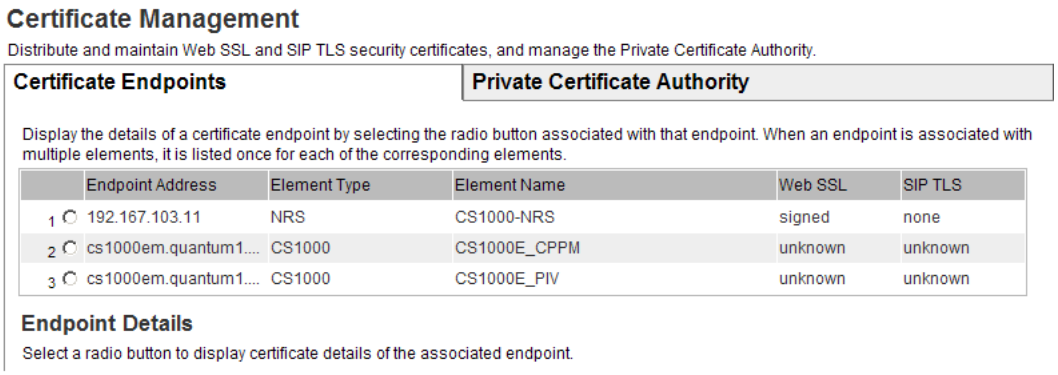
Prerequisites

- Before you can complete the steps in this procedure, you must export a certificate and its key using the steps in Exporting the current certificate and its private key by using UCM on page 145, 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 22: Status types for certificate endpoints on page 92.

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

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

   The Certificate Management page appears.

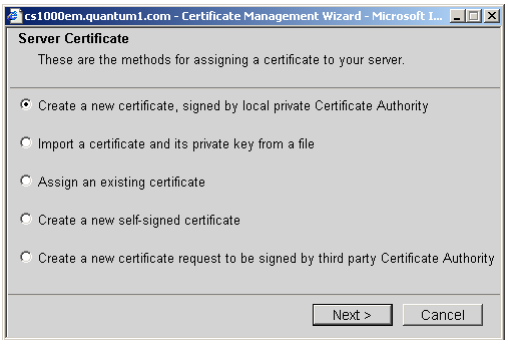


3. In the Certificate Endpoints tab, select the radio button next to the endpoint to which you want to import the certificate and key.

   The Endpoint Details section appears.

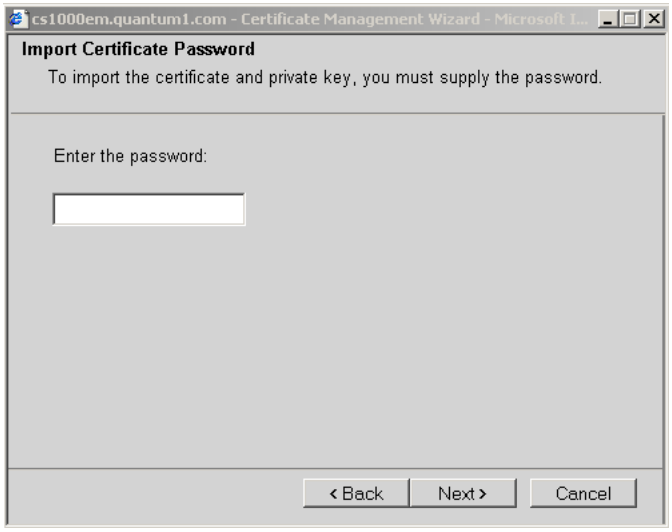
4. In the Endpoint Details pane, under Certificates, click SIP TLS or **Web SSL**.

   The Server Certificate window appears.



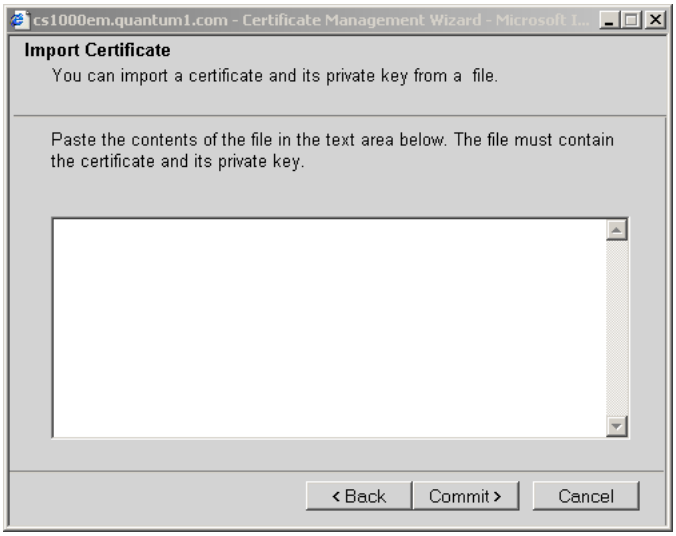
5. Select **Import a certificate and its private key from a file**, and click **Next**.

   The Import Certificate Password window appears.



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

   The Import Certificate window appears.



7. In the Import Certificate window, click in the text box, and press ctrl-v to paste the contents of the text file that you exported using the steps in Exporting the current certificate and its private key by using UCM on page 145.
8. Click **Commit**.

   The Certificate Summary window appears.
9. Click **Finish**.
10. Restart the server that you changed in this procedure.

    The changes take effect only after the server restarts.

Assign an existing certificate

Use the following procedure to assign an existing certificate to an endpoint.

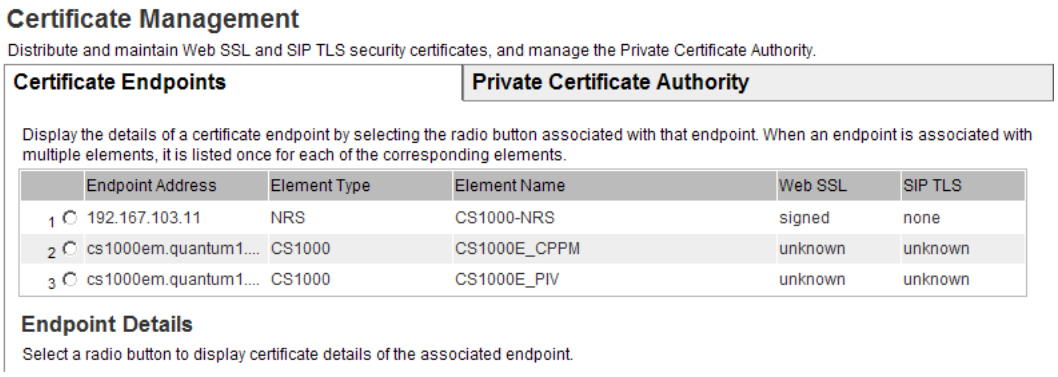
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Assigning an existing certificate by using UCM

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

   The Certificate Management page appears.



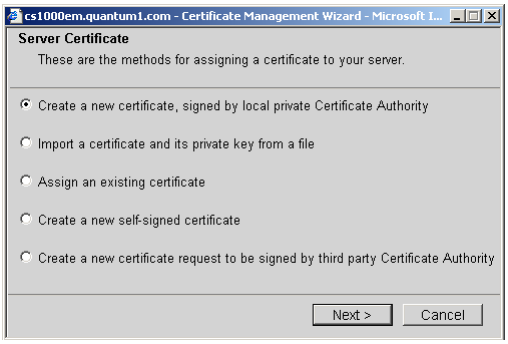
3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

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

   The Server Certificate window appears.

The Server Certificate window appears.



5. Select **Assign an existing certificate**, and click **Next**.

   The Available Certificate window appears.

6. Select a certificate from the list of available certificates, and click **Commit**.

   The Certificate Summary window appears.

7. Click **Finish**.
8. Restart the server that you changed in this procedure.

   The changes take effect only after the server restarts.

Replace the current certificate

Use the following procedure to replace the current certificate.

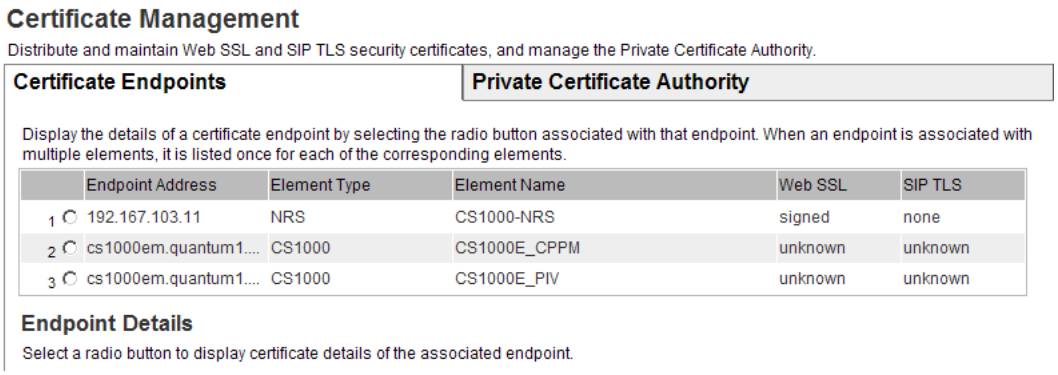
Prerequisites

- 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 22: Status types for certificate endpoints on page 92.

Replacing the current certificate by using UCM

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

   The Certificate Management page appears.



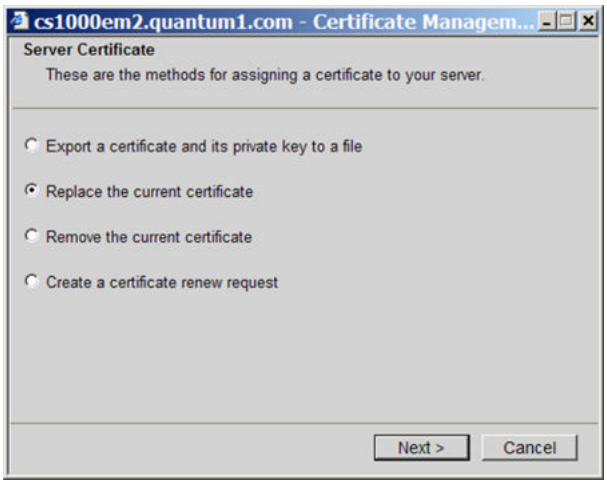
3. In the Certificate Endpoints tab, select the radio button next to the endpoint that you want to configure.

   The Endpoint Details section appears.

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

   The Server Certificate window appears.

   The Server Certificate window appears.



5. Select **Replace the current certificate**, and click **Next**.

   The Available Certificate window appears.

6. Select a certificate from the list, and click **Commit**.

The Certificate Summary window appears.

7. Click **Finish**.

Remove the current certificate

Use the following procedure to remove the current certificate.

Important:

Web SSL and SIP TLS can be disrupted if no certificate is present. Therefore, if you remove the current certificate, you must replace it or install a new one to prevent an interruption of service.

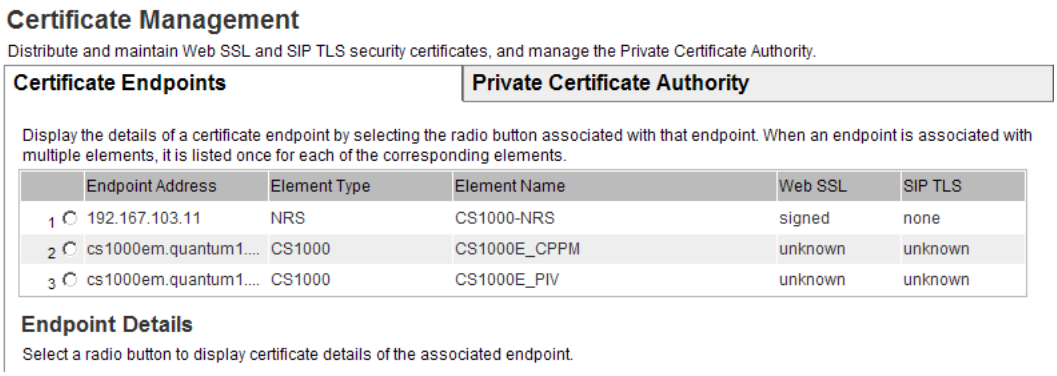
Prerequisites

- Before you remove the current certificate, ensure that the certificate endpoint status is one of: signed, self-signed, expired, or about to expire. For more information about certificate endpoint status types, see Table 22: Status types for certificate endpoints on page 92.

Removing the current certificate by using UCM

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

   The Certificate Management page appears.



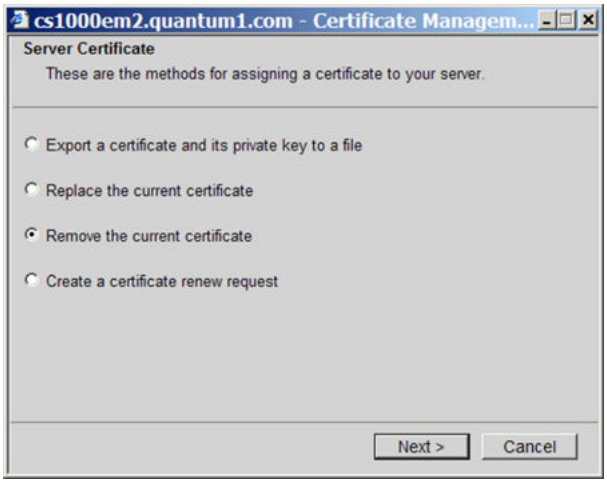
3. In the Certificate Endpoints tab, select the radio button next to the endpoint you want to configure.

   The Endpoint Details section appears.

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

   The Server Certificate window appears.

   The Server Certificate window appears.



5. Select **Remove the current certificate**, and click **Next**.

   The Remove a Certificate window appears.

6. Click **Finish**. The following message appears: `Web SSL and SIP TLS can be disrupted if no certificate is present. Therefore, if you remove the current certificate, you must replace it or install a new one to prevent an interruption of service.`

Revoke a certificate

Use the following procedure to revoke a certificate.

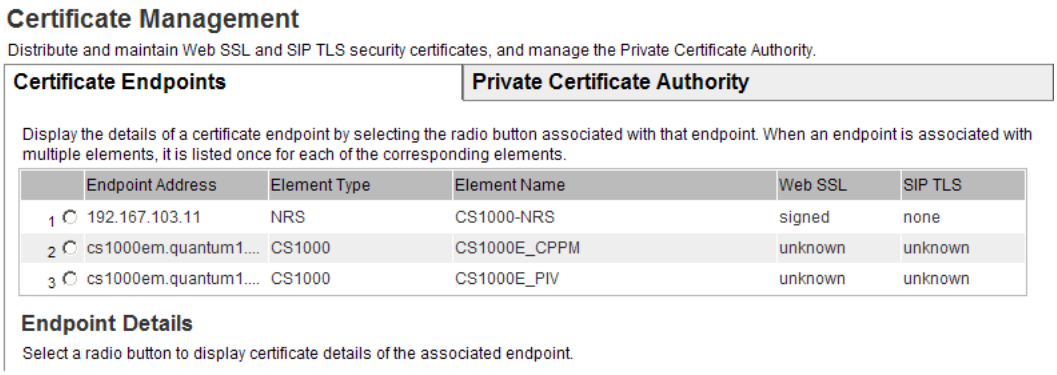
Prerequisites

- You must have SecurityAdministrator privileges.

Revoking a certificate

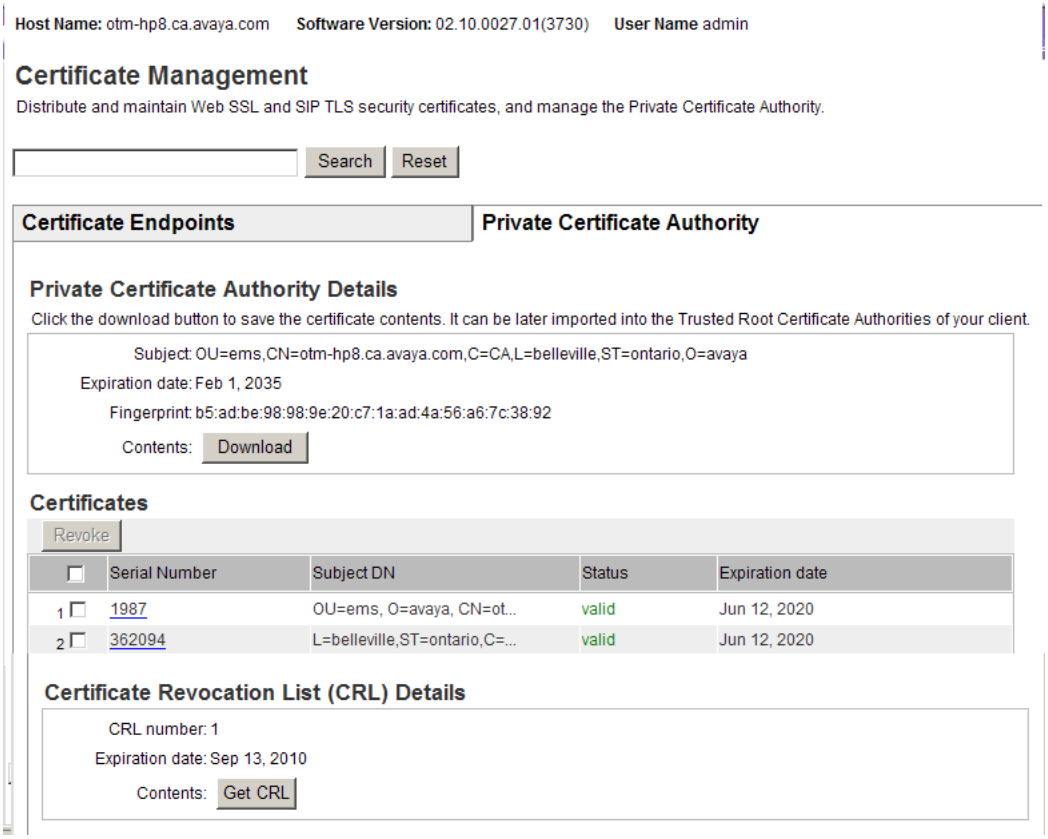
1. Log on to the UCM framework as a security administrator.
2. In the navigation tree, click Security > Certificates .

   The Certificate Management Web page appears.



3. Click the Private Certificate Authority tab.

   The Private Certificate Authority page displays.



4. In the Certificates section, select one or more of the check boxes and click Revoke to revoke the selected certificates.

Download the Certificate Revocation List (CRL) Details

Use the following procedure to download the Certificate Revocation List (CRL) Details.

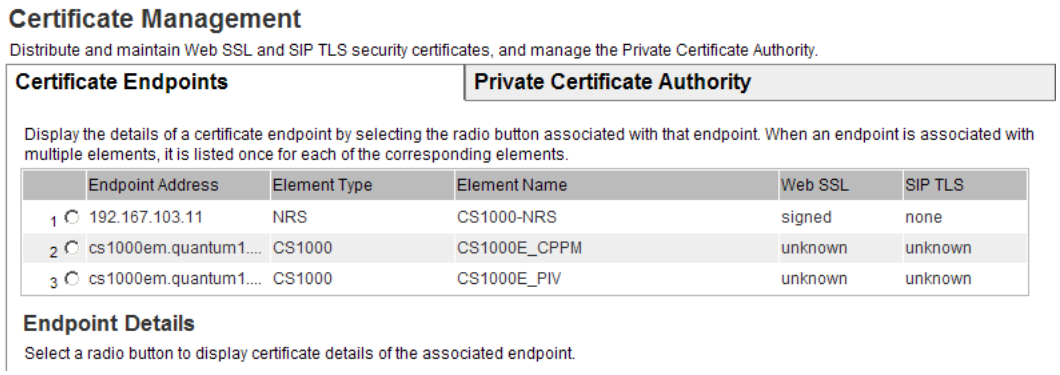
Prerequisites

- You must have SecurityAdministrator privileges.

Downloading the Certificate Revocation List (CRL) Details

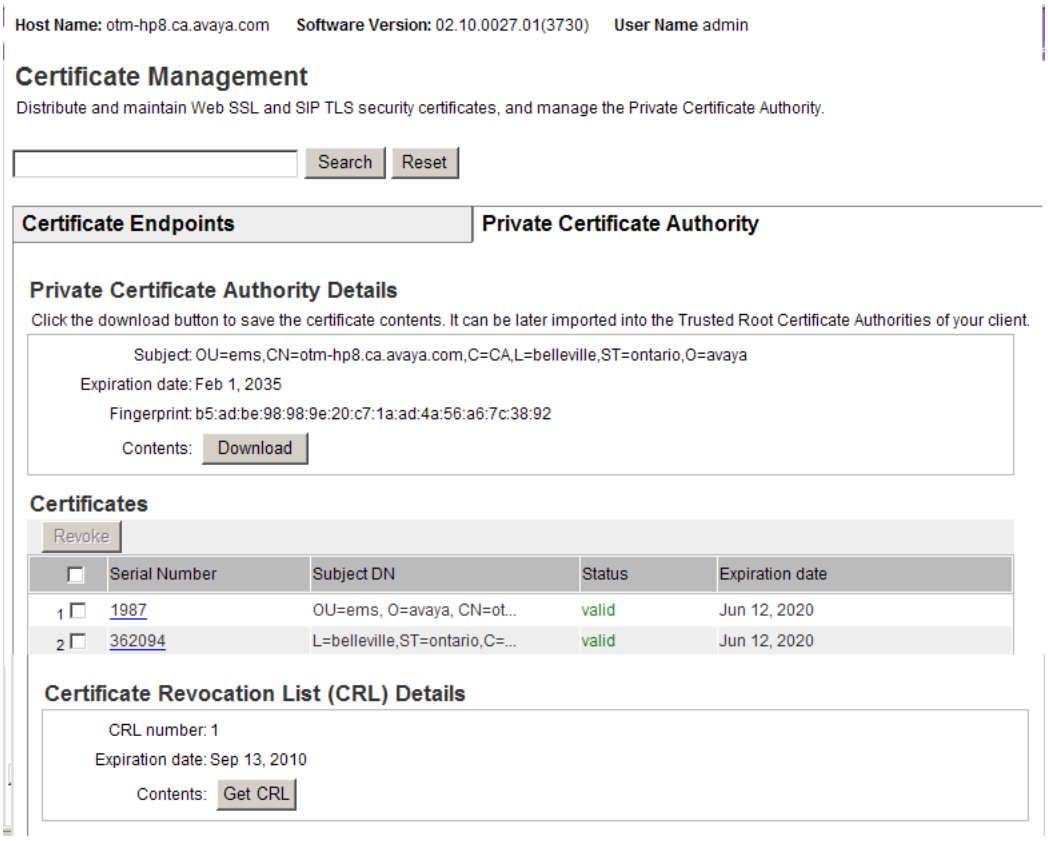
1. Log on to the UCM framework as a security administrator.
2. In the navigation tree, click Security, Certificates.

   The Certificate Management Web page appears.



3. Click the Private Certificate Authority tab.

   The Private Certificate Authority page displays.



4. In the Certificate Revocation List (CRL) Details section, click Get CRL..
   The File Download window appears.
5. Click Save.

Chapter 8: SIP security

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

About TLS security for SIP trunks

TLS protects SIP signaling traffic, providing message confidentiality and integrity in transit, as well as client-server authentication. Use the procedures in this section to configure SIP TLS on your system. For more information about SIP TLS concepts and implementation on Avaya Communication Server 1000 (Avaya CS 1000), see TLS security for SIP trunks concepts on page 42.

Certificates are deployed from the primary security server to the primary and secondary NRS servers and to the SIP endpoints. TLS communication can then be enabled between the active NRS server and the SIP endpoints. For an illustration of the distribution of certificates and subsequent TLS communication within a security domain, see Figure 14: SIP TLS with one security domain on page 159.

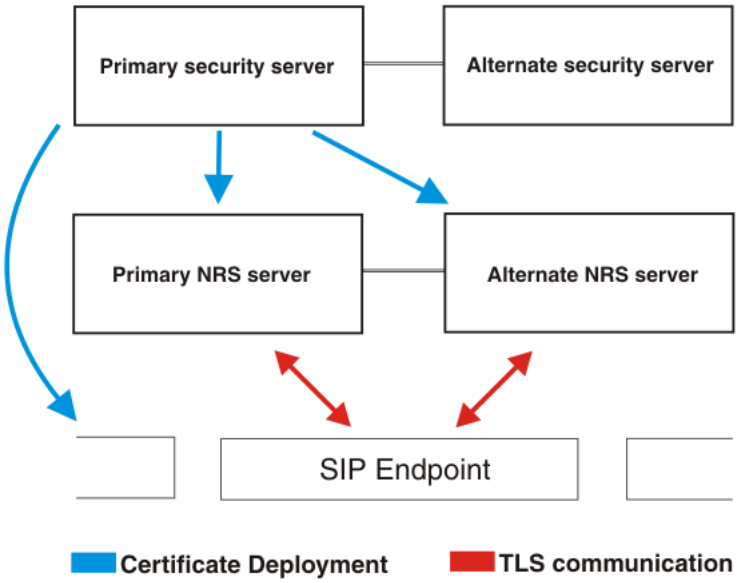


Figure 14: SIP TLS with one security domain

To allow TLS communication between nodes on different security domains, you must add the Certificate Authorities (CA) for all of the security domains to the trusted CA list for each node that you want to allow to communicate using TLS. For an illustration of the distribution of CAs and subsequent communication between security domains, see Figure 15: SIP TLS with multiple security domains on page 159.

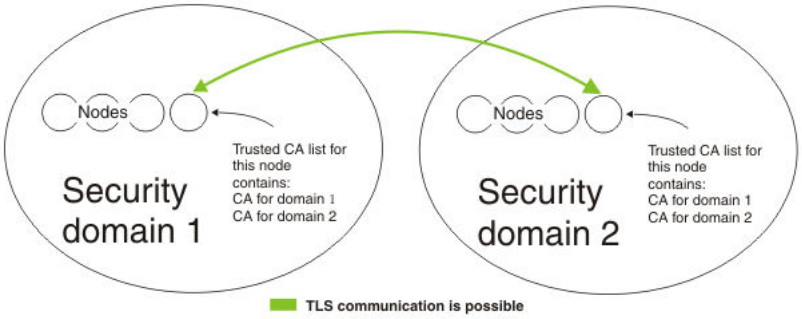


Figure 15: SIP TLS with multiple security domains

SIP Lines

SIP Lines operate similar to SIP trunks, however certificate installation for supported phone devices depends upon the specific device. For SIP Lines, the SIP Line Gateway (SLG) is updated with a certificate as opposed to the SIP Gateway used for SIP trunks.

For information about SIP Lines, see *Avaya SIP Line Fundamentals, NN43001-508*.

SIP TLS configuration overview

A typical deployment of a SIP-enabled Communication Server 1000 IP Peer network using SIP signaling consists of a Linux-based SIP Proxy and Redirect server or Linux-based NRS zone. Each such zone consists of one primary NRS, one secondary NRS, and multiple SIP gateway endpoints. The system must also include an Element Manager on Unified Communications Management that is the primary security server, and all the NRS must be members of the Unified Communications Management community of trust of that primary Unified Communications Management security server.

In the following example, you can use either SIP Proxy and Redirect servers or SIP endpoints as the system element. To configure SIP TLS, you must carry out the following four tasks.

1. Deploy certificates for SIP Proxy and Redirect server
   - In Unified Communications Management, create a certificate by using the steps in one of the following:
     - Create a certificate for SIP TLS signed by the private CA on page 111
     - Create a certificate for SIP TLS signed by a public CA on page 115
     - Create a self-signed certificate for SIP TLS on page 135
   - If the system has a secondary NRS with SIP Proxy and Redirect server:
     - In Unified Communications Management, select the server you configured in the steps above and export the certificate and the private key to a file by using the steps in Export the current certificate and its private key on page 145.
     - In Unified Communications Management, select the server to which you want to add the certificate, and Import a certificate and its key by using the steps in Import a certificate and its private key from a file on page 147.
     - In Unified Communications Management, add a CA to the service, and paste the certificate information by using the steps in Add a CA to an endpoint on page 88.
2. Enable TLS for SIP Proxy and Redirect server
   - If there is a firewall between the Unified Communications Management primary security server and the SIP Proxy and Redirect server, open the ports on the firewall to allow certificate communication, as follows:
     - TCP port 5061 for SIP TLS communication
     - UDP port 500 for IPsec Internet Key Exchange (IKE)
     - Protocol 50 for IPsec Encapsulated Payload Protocol (ESP)
     - TCP port 22 for SSH
     - TCP port 80 for HTTP
     - TCP port 443 for HTTPS
     - TCP port 58080 for SAML
     - TCP port 58081 for SAML secure mode

- TCP port 636 for LDAPS
- TCP port 15080 for Xmsg (only required if ISSS/IPsec disabled)

- Complete the following steps only once for the system. You do not need to repeat them each time you configure TLS for a SIP endpoint:
  - In Unified Communications Management, provision a public-key certificate for the primary SIP Proxy and Redirect server
  - In Unified Communications Management, provision a public-key certificate for the secondary SIP Proxy and Redirect server
  - In NRS Manager, enable SIP Proxy to open TLS ports by using the information in *Avaya Network Routing Service Fundamentals, NN43001-130*.
  - Restart the SIP Proxy service.

3. Deploy certificates for SIP endpoints
   - In Unified Communications Management, create a certificate by using the steps in one of the following:
     - Create a certificate for SIP TLS signed by the private CA on page 111
     - Create a certificate for SIP TLS signed by a public CA on page 115
     - Create a self-signed certificate for SIP TLS on page 135
   - If the system has other signaling servers running standby SIP services, you must perform the following steps for each signaling server:
     - In Unified Communications Management, select the server you configured in the steps above and export the certificate and the private key to a file by using the steps in Export the current certificate and its private key on page 145.
     - In Unified Communications Management, select the server to which you want to add the certificate, and Import a certificate and its key by using the steps in Import a certificate and its private key from a file on page 147.
     - In Unified Communications Management, add a CA to the service, and paste the certificate information by using the steps in Add a CA to an endpoint on page 88.
4. Enable TLS for SIP endpoints
   - If there is a firewall between the Unified Communications Management primary security server and the SIP endpoint, open the ports on the firewall to allow certificate communication, as follows:
     - TCP port 5061 for SIP TLS communication
     - TCP port for IPsec
     - TCP port 22 for SSH
     - TCP port 80 for HTTP
     - TCP port 443 for HTTPS
     - TCP port 58080 for SAML

- TCP port 58081 for SAML secure mode
- TCP port 636 for LDAPS
- TCP port 15080 for Xmsg

- In Element Manager, provision a SIP gateway to use TLS as transport protocol, save and transfer the changes, and restart the SIP Gateway by using the steps in Configuring SIP TLS security policy on page 164.

Use the command line interface (CLI) commands in SIP TLS maintenance using CLI on page 168 to check the configuration and status of the SIP/TLS connection.

View SIP TLS configuration

To view the current SIP TLS configuration, or to verify changes after you complete the procedures in this section, use the following procedure to examine the config.ini file.

Viewing SIP TLS configuration

1. Log on to the SIP Gateway Signaling Server with an account that has admin2 privilege.
2. Navigate to the following directory:

   ```
   /etc/opt/nortel/sigServerShare/config
   ```

3. Using a text editor, open the file **`config.ini`**.

   Job aid: config.ini on page 162 shows a sample config.ini file.

Job aid: config.ini

The following is a sample of the SIP GW security configuration settings stored in the config.ini file:

```
[SIP GW Settings]
PrimaryProxyPort=5061
PrimaryProxyTransport=TLS
SecondaryProxyPort=5061
SecondaryProxyTransport=TLS
securityPolicy=1
tlsSecurityPort=5061
clientAuthenticationEnabled=0
numByteRenegotiation=20000000
x509CertAuthenticationEnabled=0
```

The security values stored in the config.ini file are explained in Table 23: SIP TLS security parameters on page 163.

Table 23: SIP TLS security parameters

Parameter	Possible settings in Element Manager	Corresponding values in the config.ini file	Description
securityPolicy (Security Policy)	Security Disabled (Default) Best Effort Secure Local Secure End to End	0 = Security Disabled (Default) 1 = Best Effort 2 = Secure Local 3 = Secure End to End	Specify the security policy SIP TLS uses. For a description of each security policy, see Table 24: Job aid: SIP TLS security policy descriptions on page 166.
tlsSecurityPort (TLS Security Port)	A value in the range 1-65 535	Default value is : 5061	Enter the listening port that is used by TLS.
clientAuthenticationEnabled (Client Authentication)	Cleared / checked	0 = Disabled (Default) 1 = Enabled	Enable this option if you want both sides to authenticate; when it is disabled, authentication is one-way. If you enable this option, sessions require greater overhead.
numByteRenegotiation (Re-negotiation)	Cleared / checked	0 = Disabled 20 000 000 = Enabled (Default)	Enable this option if you want the session key used the SIP TLS connection to be renegotiated periodically. The default is Enabled; renegotiation is triggered after 20 000 000 bytes have passed over the connection.
x509CertAuthentication (X.509 Certificate Authentication)	Cleared / checked	0 = Disabled (Default) 1 = Enabled	Enable this option to cause SIP TLS to provide both encryption and identity verification. Disable this option to allow the system, when operating on the client side of the SIP/TLS connection, to accept self-signed certificates from the server side. If you disable x509CertAuthentication, the system provides encryption only (it does not verify identity).

TLS security for SIP trunks configuration using Element Manager

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

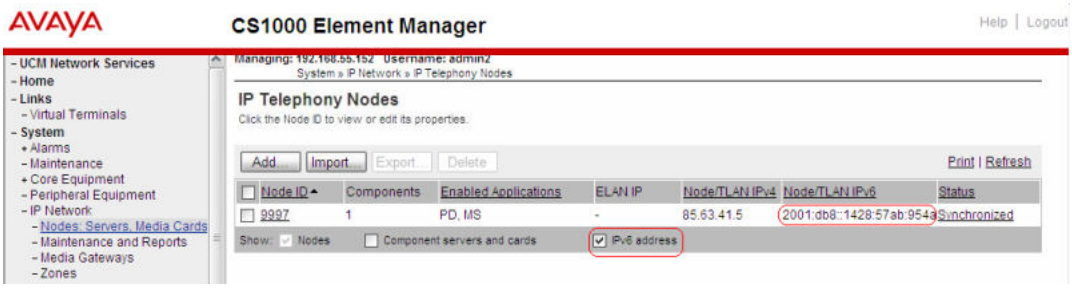
Configuring SIP TLS security policy

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

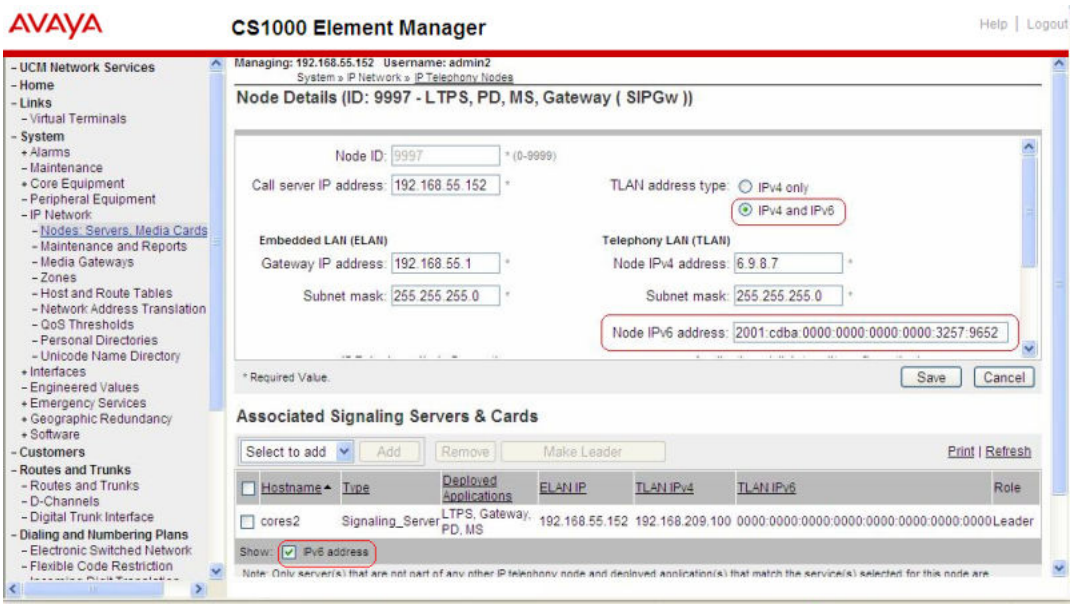
Transport Layer Security (TLS) should be configured as TLS never or TLS always. TLS always is also referred to as end-to-end TLS. Best effort TLS is not supported between CS 1000 and Avaya Aura® environments.

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

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

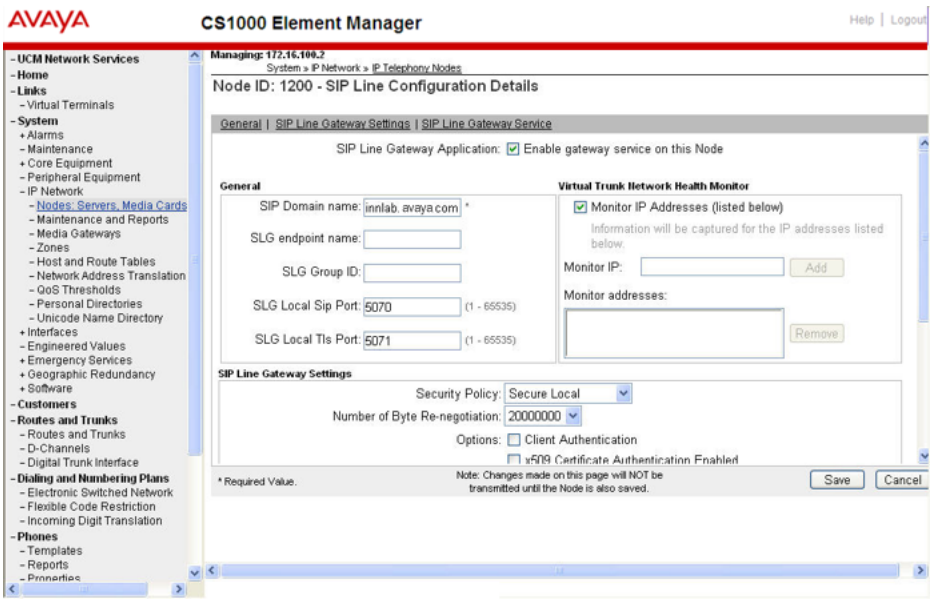


3. Click a Node ID to view the node properties.. The Node Details page appears.



4. Under Applications, click **SIP Line**.

   The SIP Line Configuration Details screen appears.



5. In the General section, in the **SLG Local Tls Port** field, type `5061`.

   For more information about TLS parameters, see Table 23: SIP TLS security parameters on page 163.

6. In the SIP Line Gateway Settings section, select a security policy from the **Security Policy** list menu. The options are as follows:

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

   For more information about available security policies, see Table 24: Job aid: SIP TLS security policy descriptions on page 166.

7. Optionally, select the **X509 Certificate Authentication** check box to enable X509 Certificate Authentication.

   Important:

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

8. Optionally, select the **Client Authentication** check box to enable Client Authentication.
9. Click **Save**.

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

10. Click **OK**.

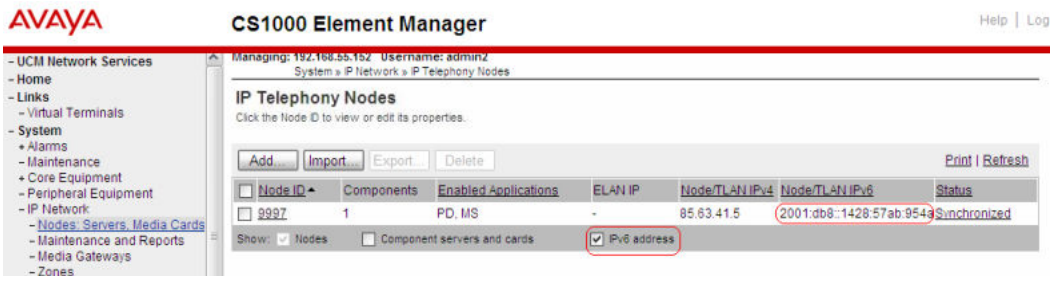
The security policy options for SIP TLS are described in Table 24: Job aid: SIP TLS security policy descriptions on page 166.

Table 24: Job aid: SIP TLS security policy descriptions

Security policy	Requirements
Security Disabled (No SIP TLS security)	Security Disabled turns SIP TLS off. SIP Gateway will listen on its TCP and UDP ports. Transport protocol to SIP Proxy or Redirect Server (for example, SIP Proxy and Redirect Server on Linux, and SIP Redirect Server on VxWorks) can be TCP or UDP. SIP URI scheme is SIP.
Best Effort (Best interoperability)	Best Effort turns SIP TLS on. SIP Gateway will listen on its TLS, TCP, and UDP ports. Transport protocol to SIP Proxy and Redirect Server on Linux can be TLS, TCP, or UDP. Transport protocol to SIP Redirect Server on VxWorks can be TCP or UDP. SIP URI scheme is SIP. Best effort TLS is not supported between CS 1000 and Avaya Aura® environments.
Secure Local (Guarantee local hop TLS)	Secure Local turns SIP TLS on. SIP Gateway will listen only on its TLS port. Transport protocol to SIP Proxy and Redirect Server on Linux can only be TLS. SIP Redirect Server on VxWorks is not supported as the next hop of this SIP Gateway. SIP URI scheme is SIP.
Secure End-to-End	Secure End-to-End turns SIP TLS on. SIP Gateway will listen only on its TLS port. Transport protocol to SIP Proxy and Redirect Server on Linux can only be TLS. SIP Redirect Server on VxWorks is not supported as the next hop of this SIP Gateway. SIP URI scheme is SIPS. In order to complete a call, all SIP Gateways in the network must be configured with Secure End-to-End , and all SIP Proxy Servers on Linux must be configured to support TLS.
Note: If you use Secure End-to-End policy or Secure Local policy, Failsafe Redirect Server is not supported.	

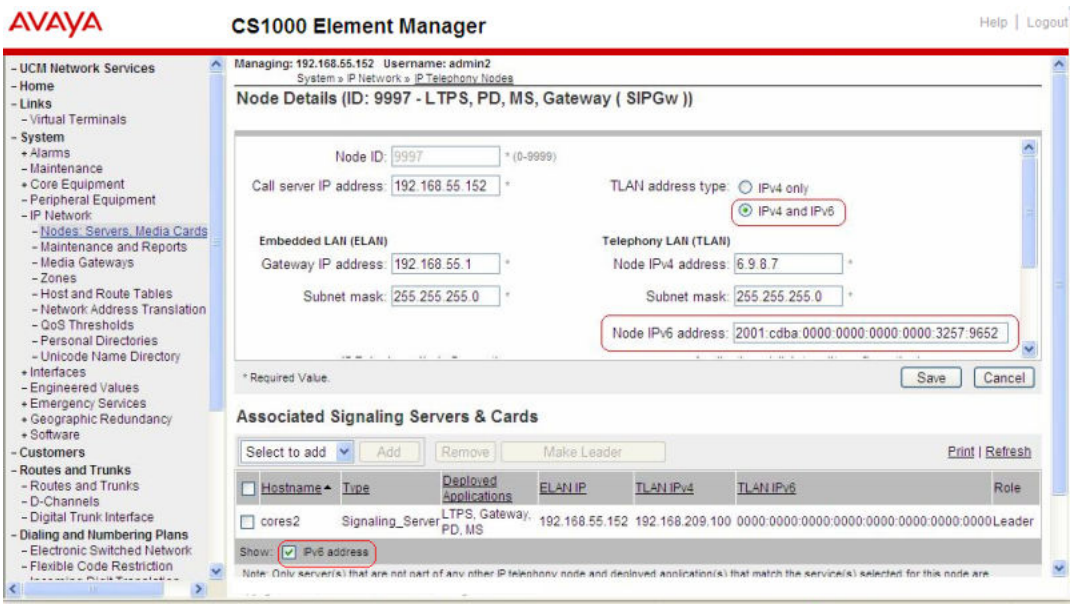
Disabling SIP TLS by using Element Manager

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



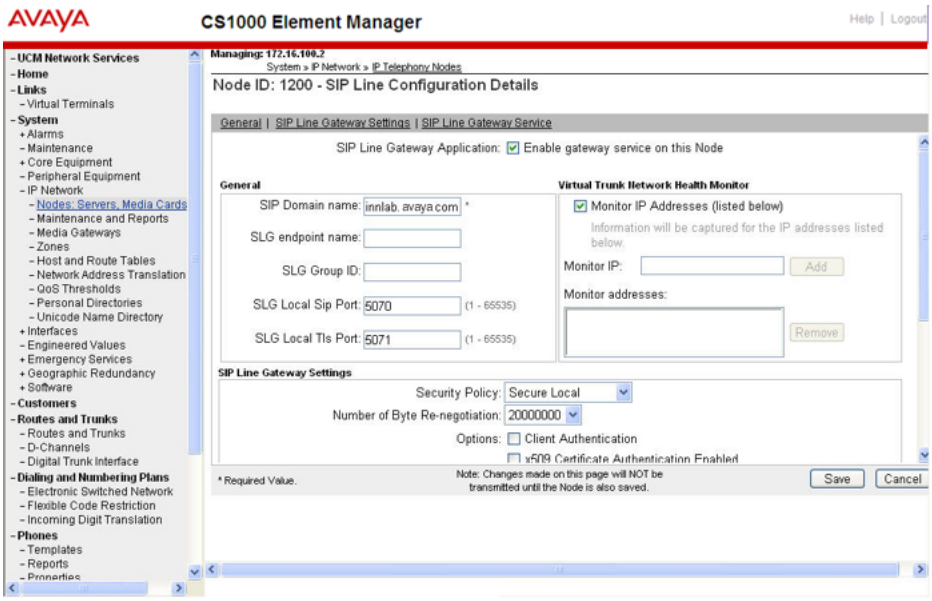
3. Click the link for the node you want to edit.

   The Node Details page appears.



4. Under Applications, click **SIP Line**.

   The SIP Line Configuration Details screen appears.



5. In the SIP Line Gateway Settings section, select Security Disabled from the **Security Policy** list menu.
6. Verify that the **SLG Local Tls Port** , **Client Authentication**, **Re-negotiation**, and **X509 Certificate Authentication** areas are cleared.

   For more information about TLS parameters, see Table 23: SIP TLS security parameters on page 163.
7. Ensure that all other fields on the page are configured with values appropriate to the SIP configuration on your system.

8. Click **Save**.

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

9. Click **OK**.

You can verify the changes by checking the config.ini file [SIP GW Settings] section. For more information about verifying SIP TLS configuration changes, see View SIP TLS configuration on page 162.

SIP TLS Certificate management

You can manage SIP TLS certificates using the Unified Communications Management (UCM) interface. For more information about certificate management using Unified Communications Management, see Certificate Management on page 85.

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 *Avaya 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.

Chapter 9: 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 Avaya Communication Server 1000 (Avaya CS 1000) through the use of Secure Real-time Transport Protocol (SRTP) on IP media paths. It applies to (Avaya CS 1000) IP Phones (Phase 2 only) and devices using DSPs (DSP daughterboard and MC32S).

With the SRTP feature you can encrypt media exchanges between two IP Phones. If you enable Media Security and a secure connection is established, IP Phones display a security icon, indicating that the leg of the call from the IP Phone to the first IP termination is secure.

Analog devices (both phones and trunks) are incapable of media encryption. Consequently, the Media Security Class of Service associated with analog devices is MSNV, for both local and SIP VTRK classes. The only exception is for local calls between IP and analog phones as these calls are encrypted when systems are configured with MSEC ON.

SRTP cannot provide Media Security for conference calls hosted through Avaya Aura® Media Server. Media Security is not supported between CS 1000 and Avaya Aura® environments. For more information about Media Security concepts and implementation on Communication Server 1000, see Media Security concepts on page 41.

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 25: Configuration options available for Media Security on page 170 shows the configuration possibilities for the Media Security feature.

Table 25: Configuration options available for Media Security

Endpoint Types	Never	Best Effort Secure IP	Always Secure IP
UNISTIM IP Phone	Y	Y	Y
TDM lines and trunks	Best Effort. No configuration option.		
VIRTUAL (SIP) Trunk (used for TDM originations)	Y	Y	N/A
SIP Endpoint	SIP Endpoint is configured in the IP Phone, not on the Call Server.		

For more information about Class of Service options for Media Security, see Table 26: Details of Class of Service options for Media Security on page 170.

Table 26: Details of Class of Service options for Media Security

Class of Service	Description
Always Secure IP (MSAW)	The IP Phone can engage in secure media exchanges only, both in the incoming and in the outgoing directions. For an outgoing call attempt, the Call Server offers Media Security to the terminator, and if the terminator accepts the offer, the media is secured by SRTP and a security icon is shown on the display, if applicable. If the terminator does not accept the offer, the call disconnects and a reorder tone sounds. The IP Phone rejects any incoming call attempt without a security offer and a reorder tone sounds.
Best Effort (MSBT)	The IP Phone can engage in secure media exchanges or insecure ones, depending on the capabilities of the IP Phone at the far end. On outgoing calls, the IP Phone attempts to originate secure calls, but falls back to RTP if the IP Phone at the far end is not capable of establishing a secure connection. If there is a security offer in the incoming call, the IP Phone accepts the offer and establishes SRTP streams; otherwise it establishes RTP streams. If applicable, icon is shown on the display when a secure connection is established.
Never (MSNV)	The IP Phone can engage in unsecured calls only. It does not propose security on outgoing calls and ignores SRTP offers for incoming calls. Use this setting if you want the IP Phone to work as it did with a previous release of CS 1000 software (for example, Release 5.5).
System Default (MSSD)	The IP Phone has a security setting as specified by the system-wide default parameter. Use this configuration option change the Class of Service settings

Table continues…

Class of Service	Description
	for a group of IP Phones, without provisioning them one at a time. The system default value is one of Always, Best Effort, or Never.

The Best Effort security setting is sufficient to suit the security needs of most users. Apply the other settings on a case-by-case basis.

UNIStim with DTLS encryption

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

To enable DTLS encryption, you must upgrade the CS 1000 system to Release 6.0 or greater and the IP Phones must have the latest firmware. You must install a DTLS certificate on CS 1000 systems and IP phones that support DTLS signaling encryption. Also, you must configure the system with at least the Basic Security level.

For more information about CS 1000 DTLS certificate creation, see Create a certificate for DTLS signed by the private CA on page 120 and Create a certificate for DTLS signed by a public CA on page 124. For more information about Private or Public CA certificate installation on IP phones, see *IP Phones Fundamentals, NN43001-368*.

Note:

This feature does not provide signaling encryption for the UFTP protocol, which is used when transferring firmware to IP Phones. Firmware data contains no sensitive information and is protected from third-party tampering by a digital signature. Notifications from the signaling server to the phones are sent using DTLS-protected UNIStim signaling to protect the signals from intercept.

The UNIStim security with DTLS feature allows the Signaling Server to detect if an IP Phone is using Secure UNIStim. You can then list IP Phones based on their employed encryption type by using the isetSecGet command on the Signaling Server or the STIP DTLS command in overlay 117 on the Call Server.

Due to the implementation of the UNIStim proxy in the Secure Multimedia Controller, it is not possible for the Signaling Server to switch the phones protected by Secure UNIStim to DTLS. You must change the action byte setting on those phones to use DTLS instead of USec, which you can do manually on the client side or by using the isetSecUpdate command on the server side.

If the configuration is provisioned to the IP Phones by DHCP or a Provisioning Server, those servers must be updated. The DTLS signaling uses different UDP ports from those used by insecure RUDP, so you must configure the network firewalls (including SMC) to allow traffic on UDP ports 4101, 7301, and 5101.

DTLS and IP Phone registration

There are two modes of IP Phone registration:

- Secure Handshake mode—the IP phone is configured to initiate a DTLS session immediately upon beginning registration.
- Switchover mode—the IP phone is configured to first establish an unencrypted RUDP session to the LTPS, then switchover to DTLS depending on the DTLS Policy

Supported hardware

UNIStim with DTLS is supported on the following Communication Server 1000 components:

- Call Servers
  - CP PIV
  - CP PM (Standalone)
  - CP PM (Co-resident)
  - CP DC (Co-resident)
  - CP MG (Co-resident)
- Signaling Servers
  - CP PM
  - CP DC
  - HP DL320 G4
  - IBM x306m
  - IBM x3350
  - Dell R300

Currently, the following IP Phones support DTLS signaling encryption (after applicable firmware upgrade):

Important:

IP Phones require UNIStim 4.0 or later to support DTLS signaling encryption.

- Avaya 1200 Series IP Deskphones (Avaya 1210/1220/1230 IP Deskphone)
- Avaya 1100 Series IP Deskphones (Avaya 1110/1120E/1140E/1150E/1165E IP Deskphone)
- Avaya 2007 IP Deskphone
- Avaya 2050 IP Softphone Release 4.0 or later

Ciphers supported by DTLS for UNIStim IP sets

The following ciphers are supported by DTLS for DTLS compatible UNIStim IP sets:

- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

From Release 7.6 SP5 onwards, DTLS supports SHA-256 ciphers .

The following table contains information about ciphers supported by each type of DTLS compatible UNIStim IP set.

Table 27: Ciphers supported by DTLS and DTLS compatible UNIStim IP sets

Cipher	Avaya 1200 Series IP Deskphones	Avaya 1100 Series IP Deskphones	2050 IP Softphones	Avaya 2007 IP Deskphone
TLS_RSA_WITH_AES_256_CBC_SHA256	X	X	X	
TLS_RSA_WITH_AES_128_CBC_SHA256	X	X	X	
TLS_RSA_WITH_AES_256_CBC_SHA	X	X	X	X
TLS_RSA_WITH_AES_128_CBC_SHA	X	X	X	X
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	X	X

Security levels

Various configuration options of UNIStim with DTLS can be combined to form three security levels: Basic, Advanced, and Complete. As the level of security increases, there are certain limitations on the supported hardware and software.

Note:

You must configure the security levels sequentially. For example, to configure or upgrade the network to Complete security, you must first enable Basic security, then upgrade to Advanced security, and then upgrade to Complete security.

Table 28: UNIStim with DTLS security levels on page 174 lists the security levels and their descriptions.

Table 28: UNIStim with DTLS security levels

Security level	Description
Basic	This level provides average signaling security when both the IP Phone and LTPS support DTLS and does not introduce any feature limitations. All features, including Virtual Office, Branch Office and Geographic Redundancy, continue to work normally as without signaling encryption. You can select this level when most CS 1000 systems on the network are upgraded to Communication Server Release 7.x and are configured for DTLS but there are systems which do not support DTLS (such as SRG or BCM) or which are not yet upgraded to 7.x. The DTLS policy on the Communication Server 1000 Release 7.x systems is configured as DTLS Best Effort. Phones are configured with action byte 1. (USec-capable phones behind an SMC may be configured with action byte 6). There is a brief period of insecure signaling at the beginning of registration.
Advanced	This level provides good security for sites requiring more than Basic security. You can use this configuration when all systems in the network are DTLS-enabled and configured as DTLS Best Effort. DTLS-capable phones are configured with action byte of 7 (regardless of whether they are behind an SMC or not). DTLS-incapable but USec-capable phones behind SMCs are configured with action byte of 6. DTLS-incapable phones which are not behind an SMC and those phones which are USec-incapable are configured with action byte of 1.
Complete	This level provides the best security for sites requiring all information on the network to be encrypted. All systems in the network are DTLS-enabled and configured as DTLS Always. All IP Phones are DTLS-capable and configured with action byte 7. Insecure registrations are not permitted.

DTLS configuration options

On the Communication Server 1000 system, DTLS-related behavior is controlled by a tri-state setting called Node DTLS Policy. This setting is configured by Line TPS node rather than on an individual system or element basis. The possible values are DTLS Off (default), DTLS Best Effort, and DTLS Always.

The DTLS policy controls which ports are open on the elements of the node and whether the elements will attempt to switch DTLS-capable phones to DTLS if they attempt to register insecurely.

Table 29: DTLS Call Server policies

	DTLS Off	DTLS Best Effort	DTLS Always
Insecure ports (4100, 7300, 5100)	Open	Open	Closed
Secure ports (4101, 7301, 5101)	Closed	Open	Open
Switchover	No switchover as DTLS is not enabled	DTLS-capable phones are switched to DTLS during registration	Registrations are only possible over DTLS, so no switchover is necessary.

All settings can be changed using the Node Properties page of Element Manager, which is accessed by navigating to **System > IP Network > Nodes: Servers, Media Cards**.

IP clients are configured with an action byte for each of the two servers (S1 and S2) to which the phone can register. The action byte dictates which protocol the phone should use to connect to the signaling server. This action byte is extended with a new value to indicate that the phone should use DTLS and should initiate a DTLS session with the server. Table 30: DTLS action byte values for IP clients on page 175 displays the possible action byte values.

Table 30: DTLS action byte values for IP clients

Action byte	Protocol stack	Note
1	UNIStim RUDP UDP	The IP Phone registers using UNIStim over RUDP, which is active over UDP. If the target LTPS node has “DTLS Best Effort” policy, the phone is switched to DTLS during registration (if it is DTLS-capable).
6	Secure UNIStim RUDP UDP	The IP Phone initiates secure UNIStim communication and establishes a secure channel with the Secure Multimedia Controller. All signaling messages, including registration messages, are protected by secure UNIStim. The LTPS detects the phones which are using Secure UNIStim and does not attempt to switch those phones to DTLS.
7	UNIStim RUDP DTLS UDP	The IP Phone initiates DTLS communication with the Signaling Server. After the DTLS session is established, the phone can register normally but uses UNIStim over DTLS. All signaling messages, including registration messages, are protected by DTLS. If the phone is configured with this action byte value, it will never be switched to Secure UNIStim or regular UNIStim.

UNIStim DTLS overlay commands

Use the STIP DTLS command in LD 117 to print information about IP Phones filtered by signaling encryption related values, including the type of connection the phone is currently using and the phones capability of making DTLS connections.

The syntax of the command is as follows:

```
STIP DTLS <NODE> <CONNECTION TYPE> <DTLS_CAPABILITY>
```

Parameter	Description
<NODE>	Node ID the phone belongs to, or use ALL to omit the node-based filtering
<CONNECTION_TYPE>	The following options are available: • INSECURE—prints the phones which are not using signalling encryption • SECURE—prints the phones which are using either USec or DTLS • DTLS—prints only the phones which are using DTLS • USEC—prints only the phones which are using UNIStim Security • ALL—prints all types of phones
<DTLS_CAPABILITY>	The following options are available: • YES—prints DTLS-capable phones • NO—prints non-DTLS capable phones • ALL—prints both DTLS and non-DTLS capable phones

You can perform mass configuration of the S1 and S2 action byte values using the Iset command **`isetSecUpdate`**. For information about Iset commands, see Table 32: Job aid: Iset commands for UNIStim DTLS on page 180.

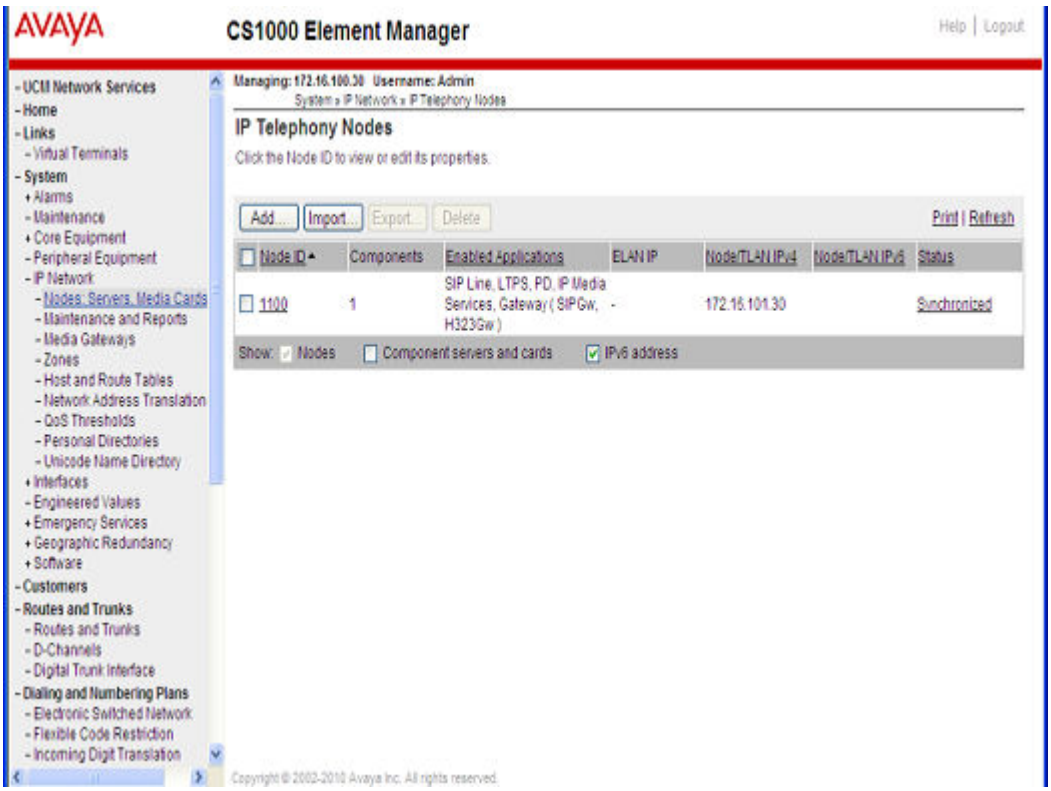
Configure UNIStim DTLS using Element Manager

Use the following procedure to configure UNIStim DTLS using Element Manager.

Configuring UNIStim DTLS using Element Manager

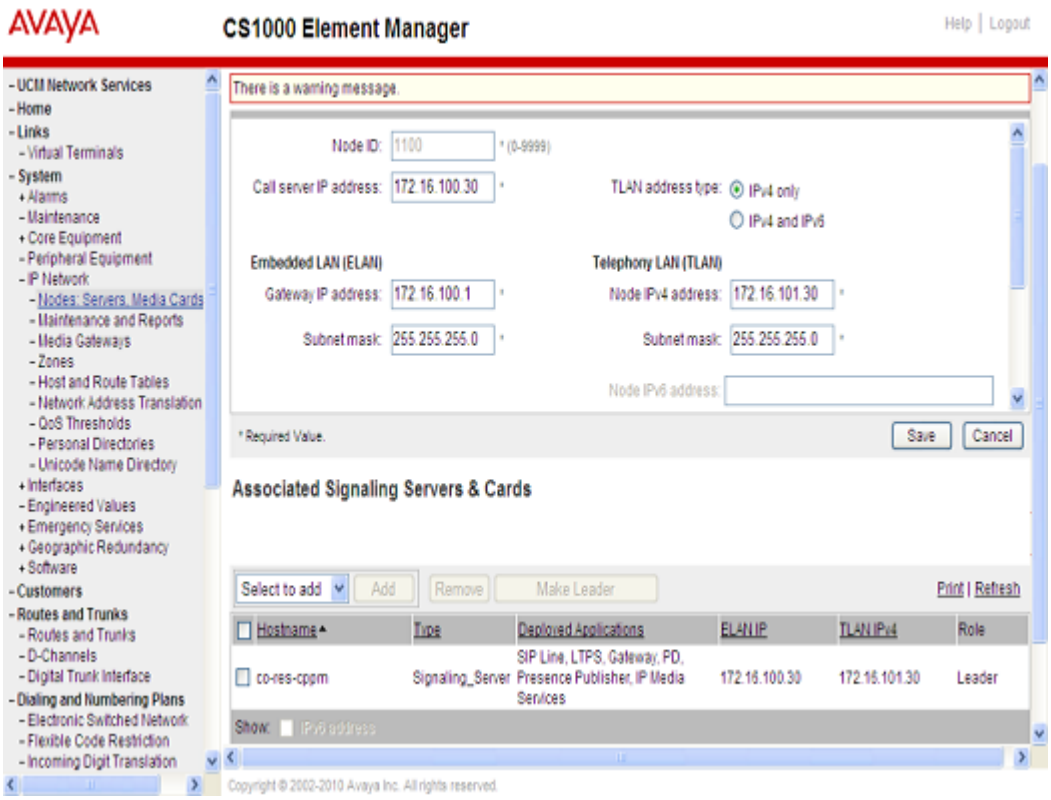
1. Navigate to **System > IP Network > Nodes: Servers, Media Cards** page.

   The IP Telephony Nodes page displays.



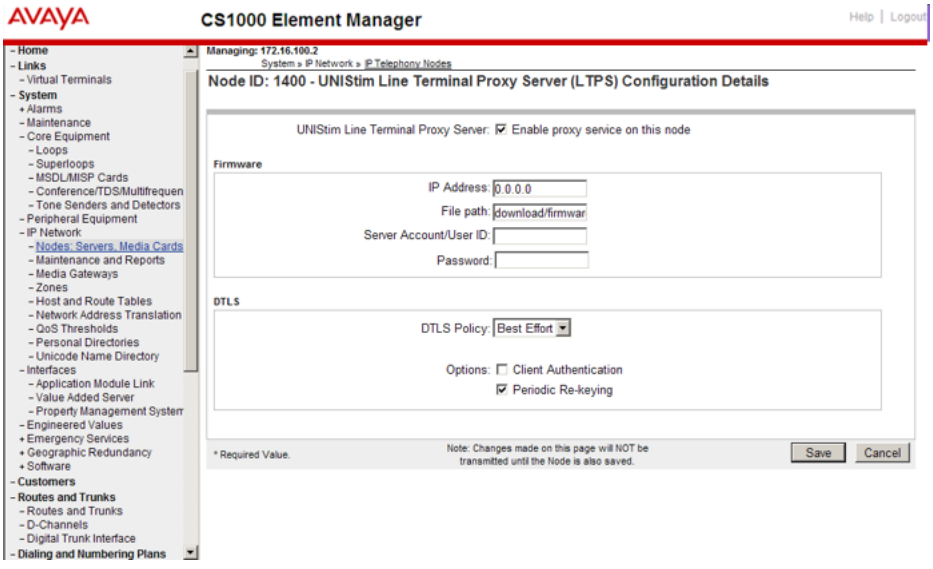
2. Click the hyperlink for the node you wish to configure.

   The Node Details page displays.



3. Click the **Terminal Proxy Server (TPS)** hyperlink.

   The Node ID * UNIStim Line Terminal Proxy Server (LTPS) Configuration Details page displays.



The following items are listed in the DTLS section of the TPS configuration page:

- DTLS Policy
- Options

4. From the **DTLS Policy** list, select the desired DTLS Policy.
5. In the Options section, select **Client Authentication** if required.

   Client Authentication determines whether the LTPS requires a certificate to be sent from the IP clients for mutual authentication. DTLS Client Authentication is supported with CS 1000 Release 7.6 Service Pack 7 or later, and UNIStim Release 5.5 Service Pack 4 or later.

   Note:

   Periodic Re-keying is not applicable for UNIStim or DTLS and any changes made to the **Periodic Re-keying** field will be ignored.
6. Click **Save**.

   The configuration changes are saved and the Node Details page displays.
7. Click **Save** to save the new configuration details for the node.

Table 31: Job aid: DTLS parameters in Element Manager Node Configuration page

Parameter	Function	Description
DTLS Policy	Enables or disables DTLS	• OFF—DTLS is not active on the node and DTLS ports are closed. • Best Effort—Both DTLS and non-DTLS ports are open on elements. The node will accept both secure and insecure registrations and will attempt to switch capable phones to DTLS. • Always—The node accepts only secure registrations. Insecure RUDP ports are not open on the node elements. It is not possible to register a DTLS-incapable phone to this node.
Client Authentication	Enables or disables Client Authentication	Select this option if you want both sides to authenticate. If you enable Client Authentication, sessions require greater overhead. To support client authentication, CS 1000 Release 7.6 Service Pack 7 or later, and UNIStim Release 5.5 Service Pack 4 or later are required. By default, the Client Authentication option is cleared. Clear the Client Authentication field when only one-way authentication is required.
Periodic Re-keying	Not applicable for UNIStim/ DTLS	-

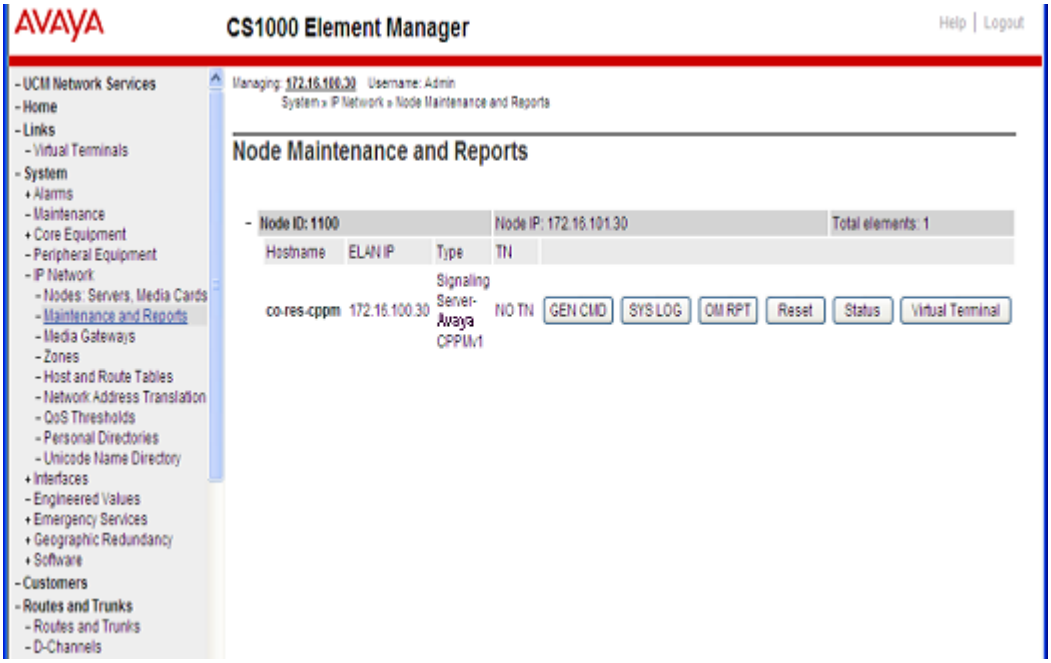
Update UNIStim DTLS using Element Manager

Use this procedure to retrieve and update the UNIStim DTLS information from an existing cluster.

Updating UNIStim DTLS using Element Manager

1. In Element Manager, navigate to **System > IP Networks > Maintenance and Reports** .

   The Node Maintenance and Reports page appears.



   You can click the **+** or **-** to expand or collapse the node details.

2. Choose the desired element and click **GEN CMD**.
3. From the Group list, select **Iset**.
4. From the Command list, select a command.

   Refer toTable 32: Job aid: Iset commands for UNIStim DTLS on page 180 for a list of iset commands and their descriptions.
5. If applicable, enter the appropriate parameters for the selected command.
6. Click **Run**.

Table 32: Job aid: Iset commands for UNIStim DTLS

Command	Description
isetSecGet	Retrieves the DTLS IP Phone details, where: • Filter = a text string of one or more of the following filtering items: - IP - Type - TN - Encryption - Action

Table continues…

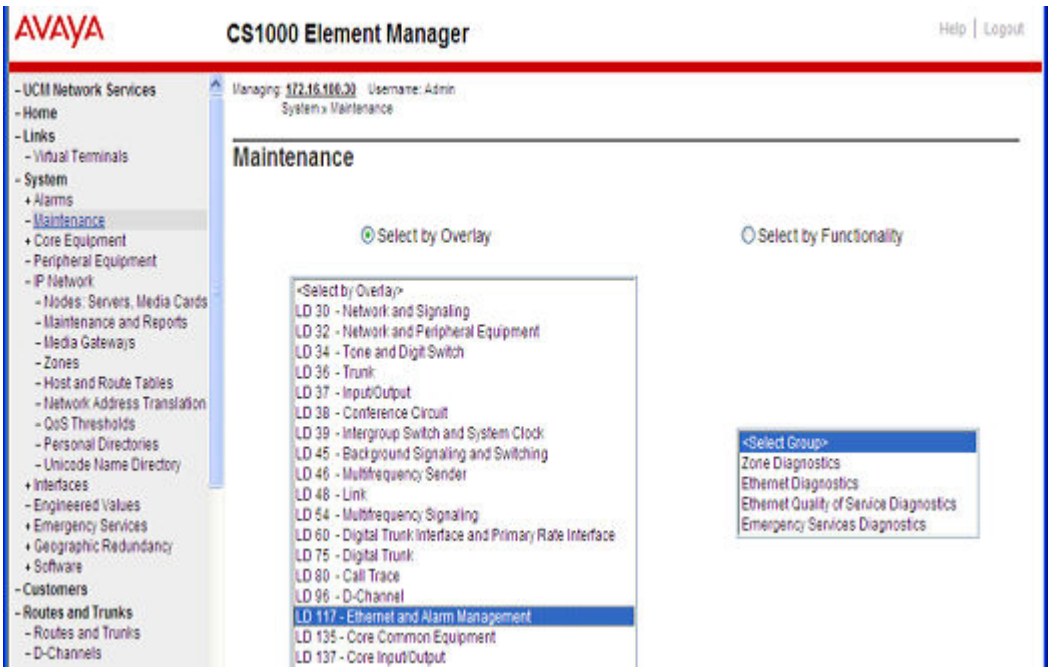
Command	Description
	- DTLSCap The filter field is limited to 80 characters.
isetSecUpdate	Reconfigures the S1 and S2 ports and action bytes on the IP Phones, where: • Filter = the same syntax as described for isetSecGet • Server ID = 1 or 2, to indicate whether S1 or S2 configurations must be updated • Action = 1, 6 or 7 • Port = the port number to be configured. The default port value is 4100 if Action is 1 or 6, and 4101 if Action is 7. Generally, it is not recommended to specify this value unless there is a need to do so. **Note:** You must restart updated IP phones for configuration changes to take effect.
isetSecShow	Prints the DTLS IP Phone details.

View UNISTIM DTLS details using Element Manager

Use this procedure to retrieve and view the UNIStim DTLS details using the Element Manager interface. This procedure uses the same query as the STIP DTLS command in LD 117.

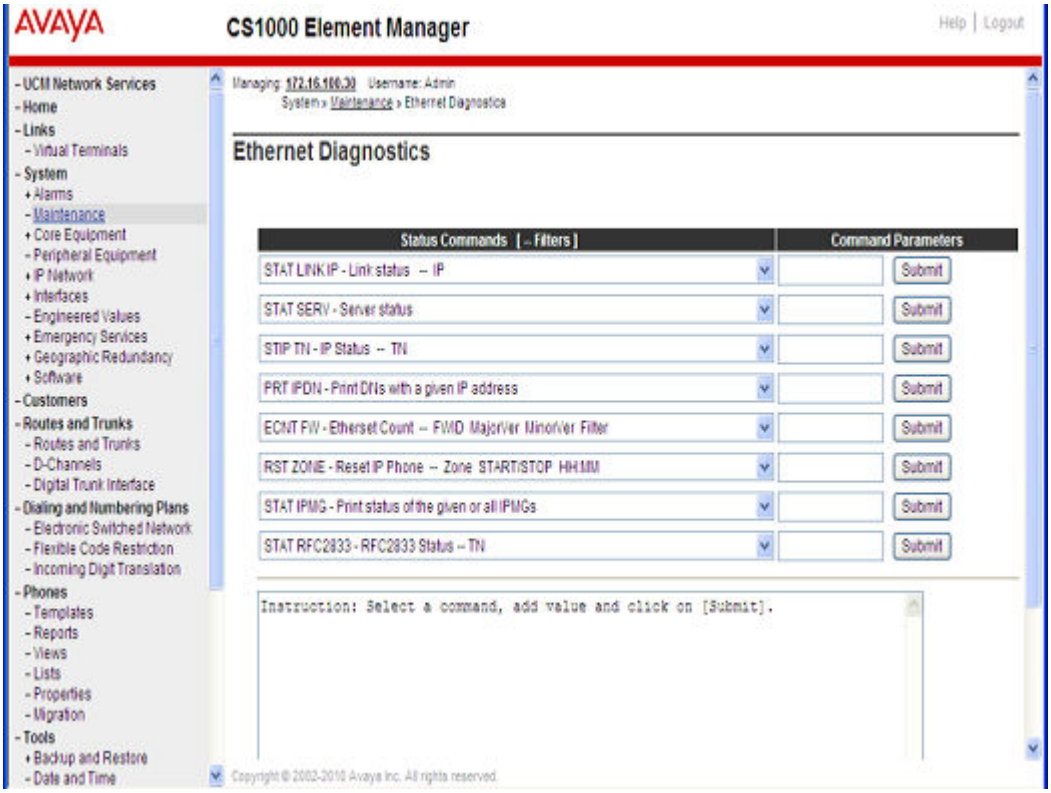
Viewing UNIStim DTLS details using Element Manager

1. In Element Manager, navigate to **System > Maintenance**.
2. From the list, select **LD117 – Ethernet and Alarm Management**.
3. From the group menu, select **Ethernet Diagnostics**.



The Ethernet Diagnostics page displays.

4. From the STIP command list, select **STIP DTLS** .



5. Enter the applicable Command Parameters.
6. Click **Submit**.

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 *Avaya 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 *Avaya IP Phones Fundamentals, NN43001-368*.

Parameters for media security configuration

The following parameters should be modified on SIP Line IP phones for configuring media security:

Parameter	Configuration	Description
SRTP_ENABLED	YES	This parameter configures SFTP configuration values. The default value is NO. Other values for this parameter: • YES – enables SRTP
SRTP_MODE	BE-2MLines	This parameter configures SFTP configuration values. The default value is BE-2MLines. Other values for this parameter: • BE-Cap Neg (MSBT) • SecureOnly (MSAW)
	BE-Cap Neg	
	SecureOnly	

Table continues…

Parameter	Configuration	Description
SRTP_CIPHER_1	AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32	This parameter configures the preferred order for SRTP cipher offers. The default value is AES_CM_128_HMAC_SHA1_80. Other values for this parameter: • AES_CM_128_HMAC_SHA1_32 • None
SRTP_CIPHER_2	AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32	This parameter configures the preferred order for SRTP cipher offers. The default value is AES_CM_128_HMAC_SHA1_32. Other values for this parameter: • AES_CM_128_HMAC_SHA1_80 • None
FAST_EARLY_MEDIA_ENABLE	NO	This parameter allows the administrator to activate and deactivate the Fast Early Media option (according to RFC 3264).

Media Security configuration using Element Manager

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

System-wide Media Security configuration

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

You can configure system-wide Media Security using the Media Configuration page in Element Manager, as shown in Figure 16: Media Security configuration on page 185. For more information about configuring Element Manager, see *Avaya Element Manager System Reference — Administration, NN43001-632*.

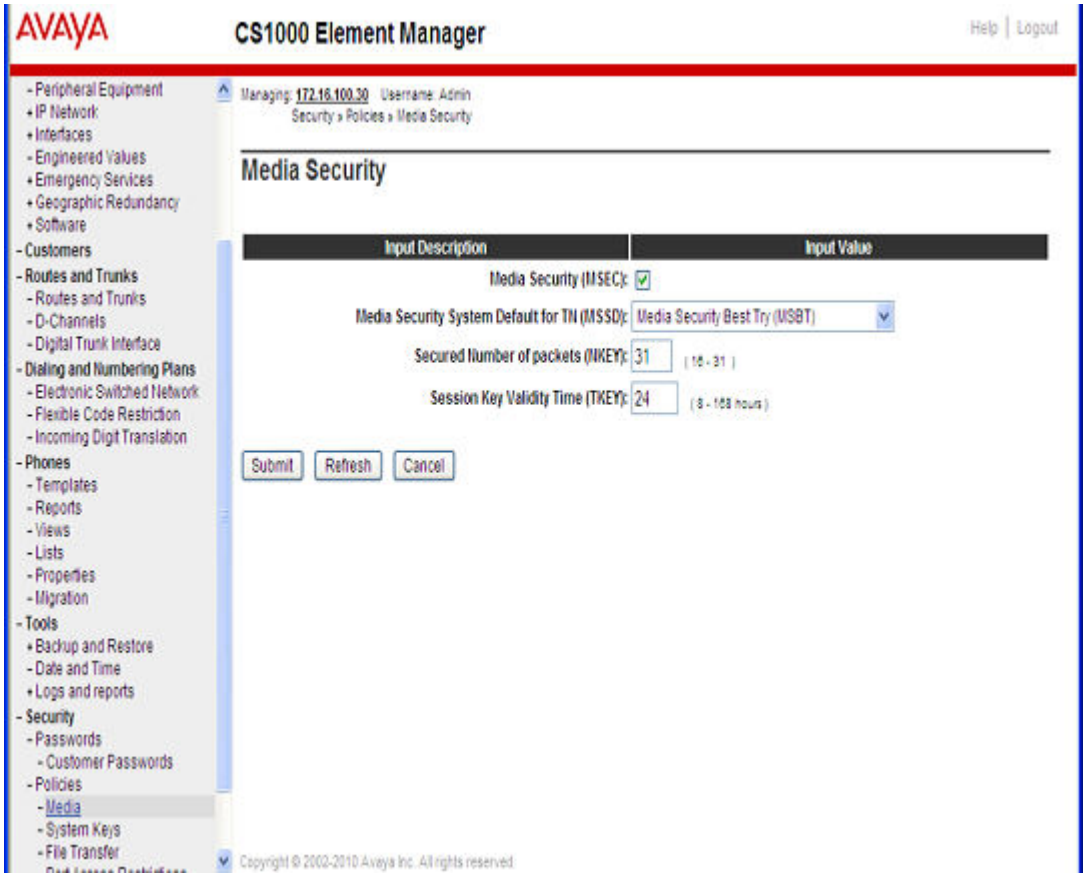
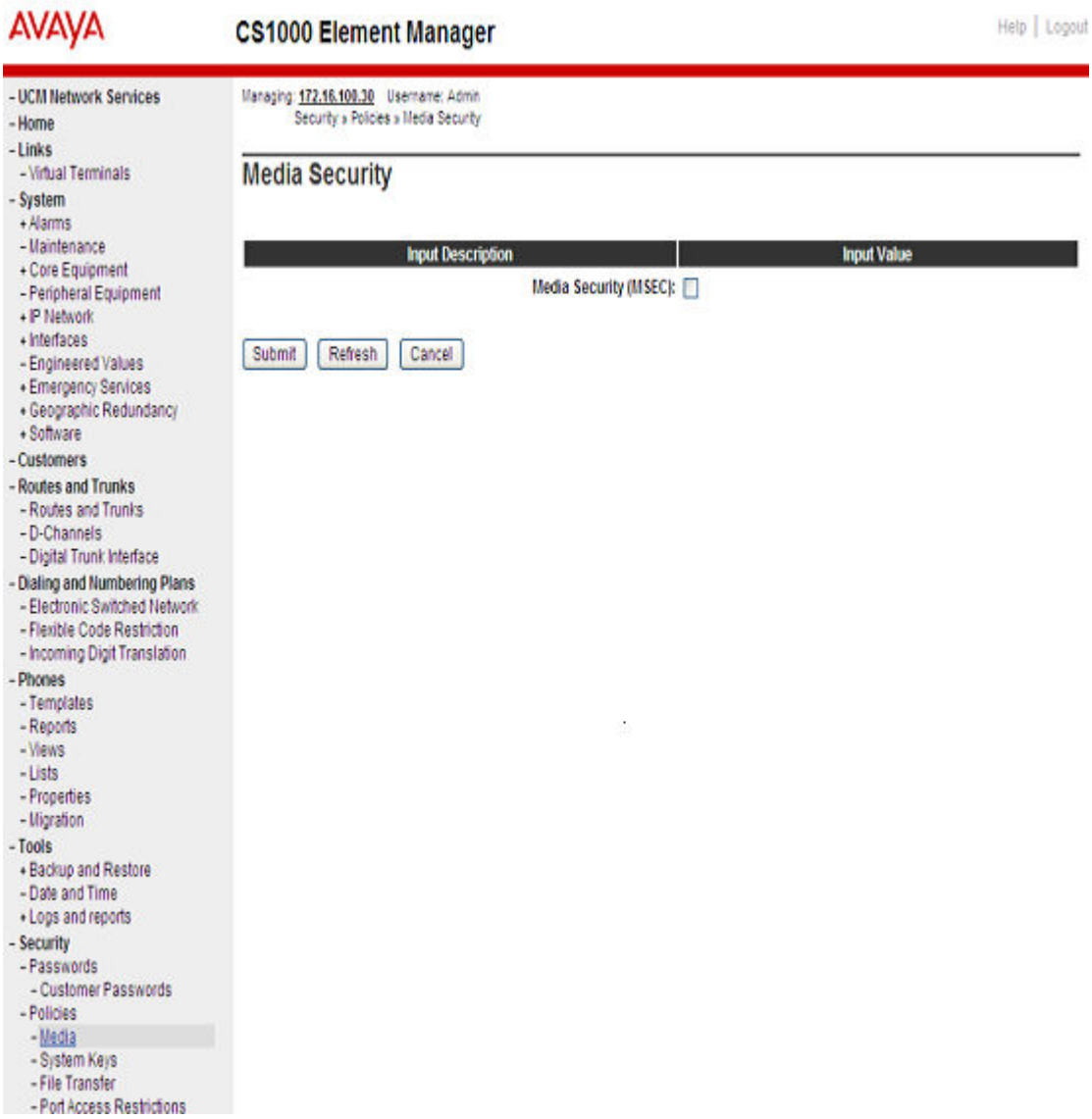


Figure 16: Media Security configuration

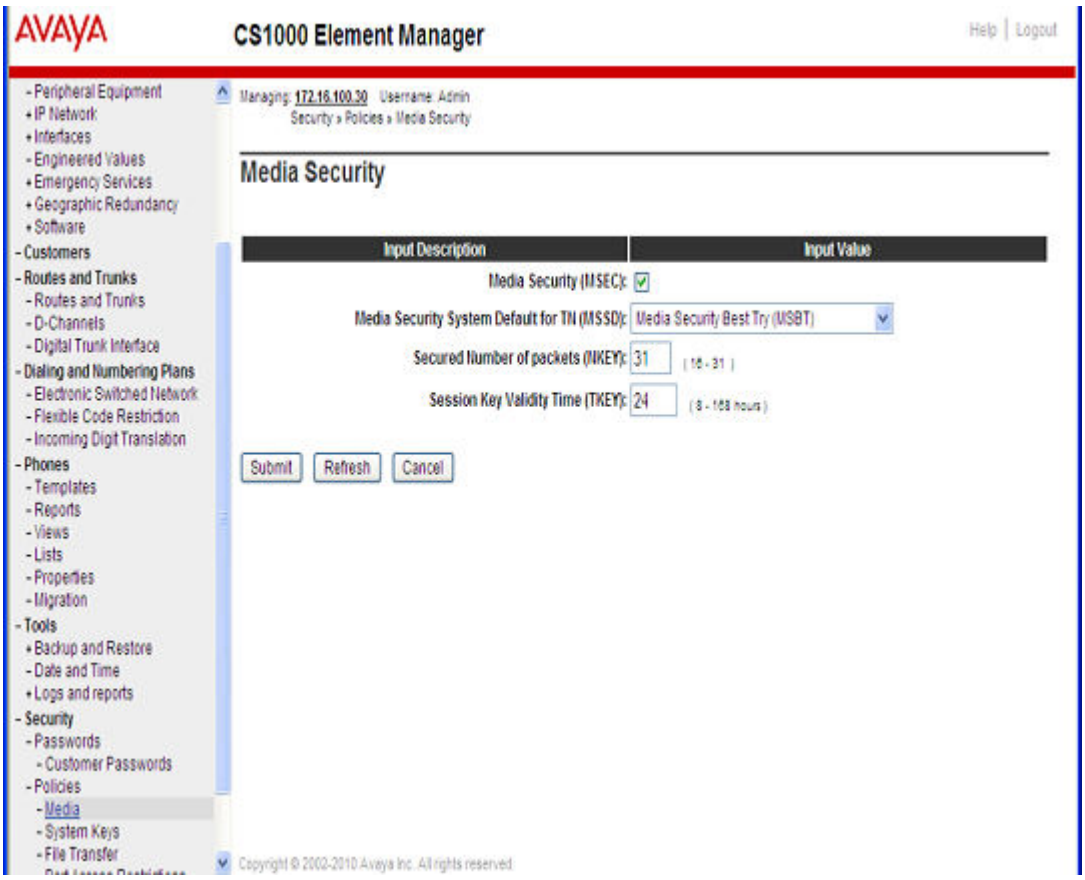
Configuring system-wide Media Security by using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click **Security > Policies > Media** .

   The Media Security page appears.



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



4. Choose one of the following options from the **Media Security System Default for TN** menu:

   MSNV to configure the Media Security default value to Never, which disables Media Security on all TNs that have the security Class of Service configured as MSSD.

   OR

   MSBT to configure the Media Security default value to Best Effort, which configures Media Security to use Best Effort on all TNs that have the security Class of Service configured as MSSD.

   OR

   MSAW to configure the system-wide default value to Always, which configures Media Security to allow secure media exchanges only. Unsecured connection attempts are blocked.

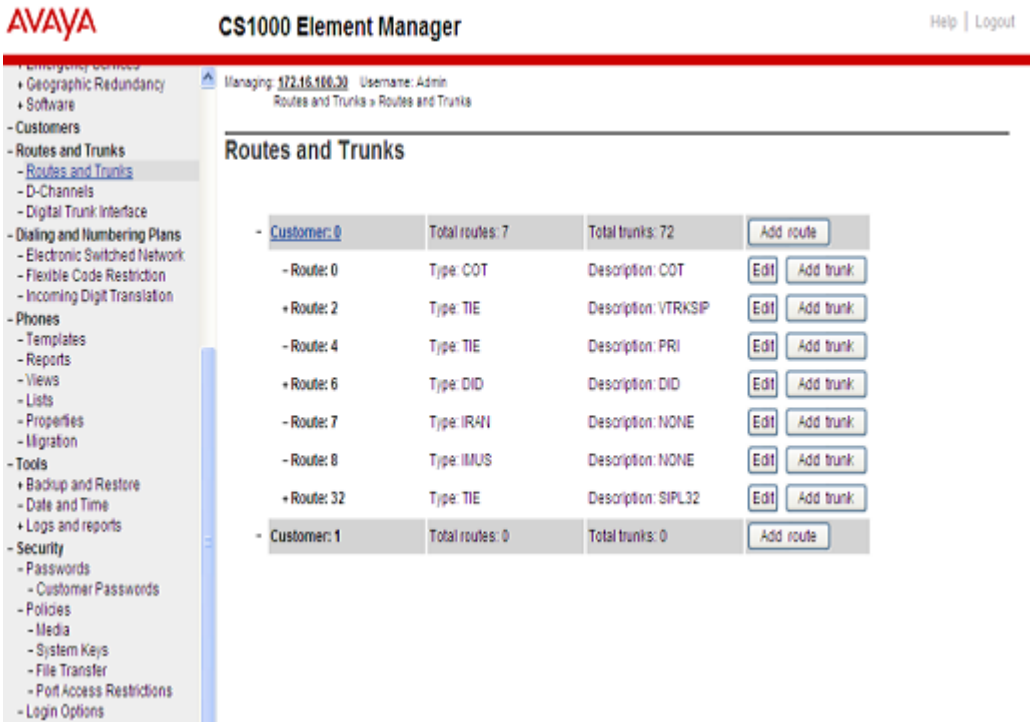
5. Enter a value in the **Secured Number of packets (NKEY)** field. The value you enter configures the number of packets a key can secure before it must be regenerated, and must be an integer in the range of 16 to 31.
6. Enter a value in the **Session Key Validity Time (TKEY)** field. The value you enter configures the maximum length of time, in hours, that a session key can remain valid, and must be an integer in the range of 8 to 168.
7. Click **Submit** to save your changes.

VTRK Class of Service configuration

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

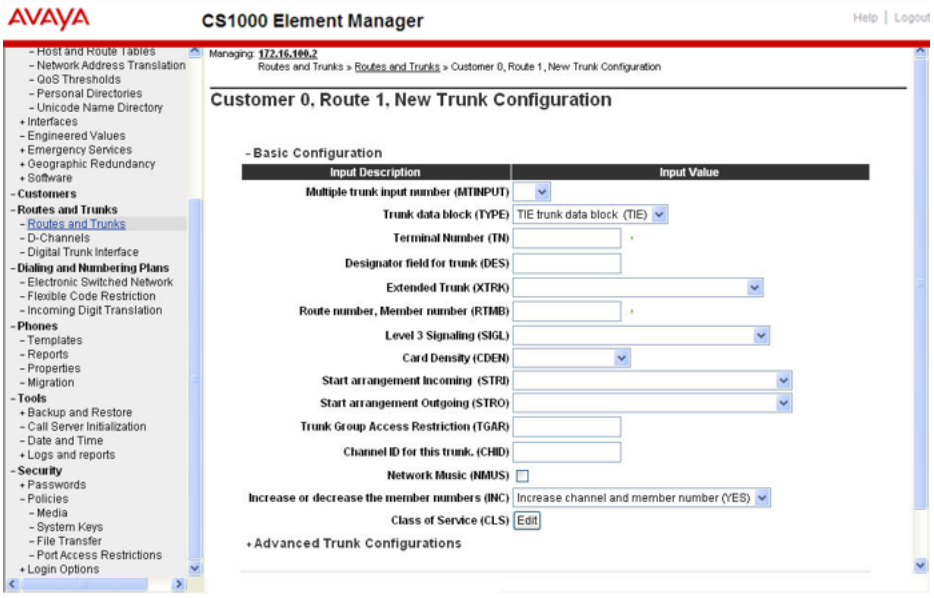
Configuring VTRK Class of Service using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click **Routes and Trunks > Routes and Trunks**, and select a customer record.



3. Click **Add Trunk** for the route to which you want to add a trunk.

   The New Trunk Configuration page appears.



4. From the **Trunk datablock type** menu, select **IP Trunk (IPT1)**.
5. Enter the terminal number of the trunk in the **Terminal Number (TN)** field.
6. Ensure that the **Extended Trunk (XTRK)** field contains a value of **VTRK**.
7. Enter the RTMB in the **Route number, Member number (RTMB)** field.
8. Click **Edit** next to **Class of Service (CLS)**.
9. In the **Media Security (CLS)** menu, select one of the following Class of Service values:

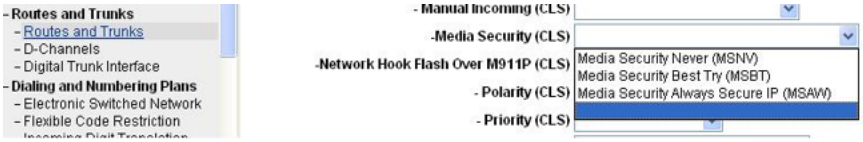
   MSNV to configure the IP Phone Media Security Class of Service to Never, which disables Media Security on the IP Phone. The system does not attempt to secure either incoming or outgoing calls.

   OR

   MSBT to configure the IP Phone Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls.

   OR

   MSAW to configure the IP Phone Media Security Class of Service to Media Security Always Secure IP.



10. Click **Return Class of Service**.
11. Click **Save**.

Media Security configuration using overlays

Use the procedures in this section to configure the Media Security feature using LD 11, 14, and 17.

System-wide Media Security configuration

You can configure a system-wide configuration setting that controls whether or not the Communication Server 1000 system provides Media Security. By default, Media Security is enabled on the system.

You can configure system-wide Media Security settings using LD 17. For more information about LD 17, see *Avaya Software Input Output Administration, NN43001-611*.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Table 33: LD 17 — Configure system-wide Media Security

Prompt	Response	Description
REQ	CHG	Change existing data block
TYPE	PARM	Data block type: System Parameters
MSEC	[ON] / OFF	Enable or disable Media Security at the system wide level for the Call Server. If ON, IP Phones with a Class of Service other than MSNV can secure calls using Media Security, as can Mindspeed DSPs. If OFF, the Media Security Class of Service settings on the IP Phones have no effect.
MSSD	[MSNV]	Media Security Never. This option disables Media Security on all IP Phones that have the security Class of Service configured as MSSD.
	MSBT	Media Security Best Effort. This option configures Media Security to use Best Effort on all TNs that have the security Class of Service configured as MSSD.
	MSAW	Media Security Always. This option configures Media Security to allow secure media exchanges only. Unsecured connection attempts are blocked.
NKEY	<NKEY>	An integer in the range of 16-31. The default value for <NKEY> is 31, providing 231 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 = 2n.
TKEY	<TKEY>	An integer in the range of 8-168.

Table continues…

Prompt	Response	Description
		This value is the maximum length of time, measured in hours, that a session key can remain valid. The default value for TKEY is 24 hours.

Class of Service configuration

Use LD 11 to assign a Media Security Class of Service for IP Phones. For more information about LD 11, see *Avaya Software Input Output Administration, NN43001-611*.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Table 34: LD 11 — Configure Media Security Class of Service for IP Phones

Prompt	Response	Description
REQ	CHG	Change record
TYPE	a...a	IP Phone type. For example, 2002P2, 2050PC, or 2004P2.
	?	Displays a list of possible responses.
TN	l s c u	Terminal number of a configured IP Phone of the selected type.
ECHG	YES	Easy Change. This allows change to any prompt in this LD without having to <CR> through all unrelated prompts. ECHG is prompted when REQ = CHG.
ITEM	CLS MSNV	Configures 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.
	CLS MSBT	Configures the IP Phone Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls.
	CLS MSAW	Configures 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.
	CLS MSSD	Configures the IP Phone Media Security Class of Service to use the system default (MSNV).

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 on page 190. 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 *Avaya Software Input Output Administration, NN43001-611*.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Table 35: LD 14 — Configure VTRK Class of Service

Prompt	Response	Description
REQ	NEW / CHG	Create or change a data block.
TYPE	IPTI	IP TIE trunk data block.
TN	l s c u	Terminal Number Loop Shelf Card Unit value.
XTRK	VTRK	Press **Enter** to accept the default value of VTRK.
CUST	xx	Customer number as defined in LD 15.
RTMB	xxx yy	Route number and Member number.
CHID	x	Channel ID for the trunk.
STRI	IMM	Immediate. The terminating trunk is not expected to return a pulse telling the originating end to begin sending digits. **Note:** If the trunk is intended for SIP DECT or Converged Office applications, enter WNK (Wink or Fast Flash) at this prompt.
STRO	IMM	Immediate. **Note:** If the trunk is intended for SIP DECT or Converged Office applications, enter WNK (Wink or Fast Flash) at this prompt.
CLS	MSNV	Configures 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.
	MSBT	Configures the VTRK Media Security Class of Service to Best Effort. The system attempts to secure both incoming and outgoing calls.

Media Security configuration information

Use the procedures in this section to access information about the configuration of the Media Security feature using overlays or from an IP Phone. For information about Media Security configuration using the Element Manager interface, see Media Security configuration using Element Manager on page 184.

Media Security configuration information available using overlays

This section provides information about tools you can use to access configuration information for Media Security.

Use the following procedure to view information about Media Security using LD 117.

Viewing Media Security Settings using LD 117

1. At the prompt, enter `PRT MSEC [ SYS | IP <ip_address> | TN <tn> | ALL ]`.

   For more information about the arguments for this command, see Table 36: Job aid: commands to access information about Media Security configuration on page 193.

Table 36: Job aid: commands to access information about Media Security configuration

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

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Viewing system-wide Media Security settings using LD 22

1. Log on to the Call Server CLI using a PWD2 account.
2. At the LD 22 `REQ` prompt, enter `PRT`.
3. At the LD 22 `TYPE` prompt, enter `PARM`.

Use the following procedure to view information about user level Class of Service using LD 11 or LD 20.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

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

1. Log on to the Call Server CLI using a PWD2 account.
2. At the LD 20 or LD 11 `REQ` prompt, enter `PRT`.
3. At the LD 20 or LD 11 `TYPE` prompt, enter `TNB`.
4. At the LD 20 or LD 11 `TN` prompt, enter *<lscu>*.
5. Press `Enter` at each subsequent prompt.

Table 37: Variable definitions

Variable	Value
<lscu>	Loop Shelf Card Unit value.

Media Security information available using an IP Phone

Use the following procedure to view the Media Security configuration of an IP Phone using the menus on the IP Phone.

Viewing Media Security information using an IP Phone

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 on page 191.
5. Press the **Cancel** soft key to return to the main menu.

SIP Route information available using overlays

Use the following procedure to view SIP Route information by using LD 21.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Table 38: LD 21 — View SIP Route information

Prompt	Response	Description
REQ	PRT	Print data block for the TYPE specified
TYPE	RDB	Route Data Block
CUST	xx	Customer number as defined in LD 15.
ROUT	x...x	Route number

Chapter 10: User and password management

This chapter contains procedures to help you manage users, passwords, and privileges. The chapter is divided into the following sections:

- Account types and roles on page 198
- User and password management using overlays on page 202
- User and password management using Element Manager on page 215

Important:

Backup and restore operations for Linux-based UCM elements involve critical data that can have possible impacts to system security. You should consider data security and accountability when assigning roles and permissions for user accounts that have backup and restore privileges. To ensure optimum security of backup data for Linux base elements Avaya recommends using the central backup and restore common service through the UCM primary server Deployment Manager, for backup and restore operations of all Linux based UCM member elements.

For maintenance procedures that require the system operator to invoke backup and restore operations locally from the Linux base UCM member element, Avaya recommends using a securely managed external sFTP server. Security auditing procedures should be implemented to verify compliance by system operators.

System operators should avoid the routine use of Linux Base Manager or Linux CLI commands to backup the Linux base UCM member element to a local removable storage device

For more information about user and password management concepts on Avaya Communication Server 1000 (Avaya CS 1000), see User and password management concepts on page 43.

For information about configuring users using Unified Communications Management, see *Avaya Unified Communications Management Fundamentals, NN43001-116*.

Note:

All user accounts created in previous releases must be recreated using Unified Communications Management in order for them to be recognized by Radius.

For VxWorks-based elements (except Call Servers), the accounts database is reset to default during the upgrade. After the upgrade, only the default accounts are in service until the element joins the UCM secure domain, at which time it receives the updated accounts database file from the Call Servers.

Roles and permissions

IP telephony systems must use UCM central authentication to manage system level OAM and PDT users and passwords. UCM features both built-in and custom roles.

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

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

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

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

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

For information about UCM built-in and custom roles, see *Avaya Unified Communications Management Fundamentals, NN43001-116*.

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

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

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

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

CS 1000 systems must be mapped to permissions on individual Linux base elements that are deployed and configured as CS 1000 system elements.

For information about role inheritance and permission mapping, see *Avaya Unified Communications Management Fundamentals, NN43001-116*.

Permission templates

The built-in permission templates list contains a listing of UCM built-in roles that are applicable to the UCM type of element whose permission mapping is being edited. For elements of type CS 1000, there is an additional template corresponding to a blank set of permissions for a CS 1000 administrative account "with specified OAM privileges".

This UCM template corresponds to the previous CS 1000 system-level OAM account with "limited access to overlays password" (LAPW). You can customize the permission templates when adding a new role.

For information about permission templates, see *Avaya Unified Communications Management Fundamentals, NN43001-116*.

Account types and roles

Each user has one of the following account types:

- PWD2 provides OAM level access that includes system security, account administration and general system administration
- PWD1 provides OAM level access that includes general system administration
- LAPW provides OAM level access that is restricted to user specified administration operations
- PDT1 provides PDT level access for expert technicians and Avaya Support group
- PDT2 provides ROOT level access for Avaya Developers

In addition to the access privileges and limitations that each account type offers, you can assign specific privileges to each user.

This chapter provides procedures to help you manage users and configure user privileges.

Account synchronization

When you add a user or change a password, the system automatically schedules an Equipment Data Dump (EDD) to update the accounts on each local device. When an EDD occurs, the system distributes the updated account files to all Voice Gateway Media Card, Gateway Controller, 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 on page 275.

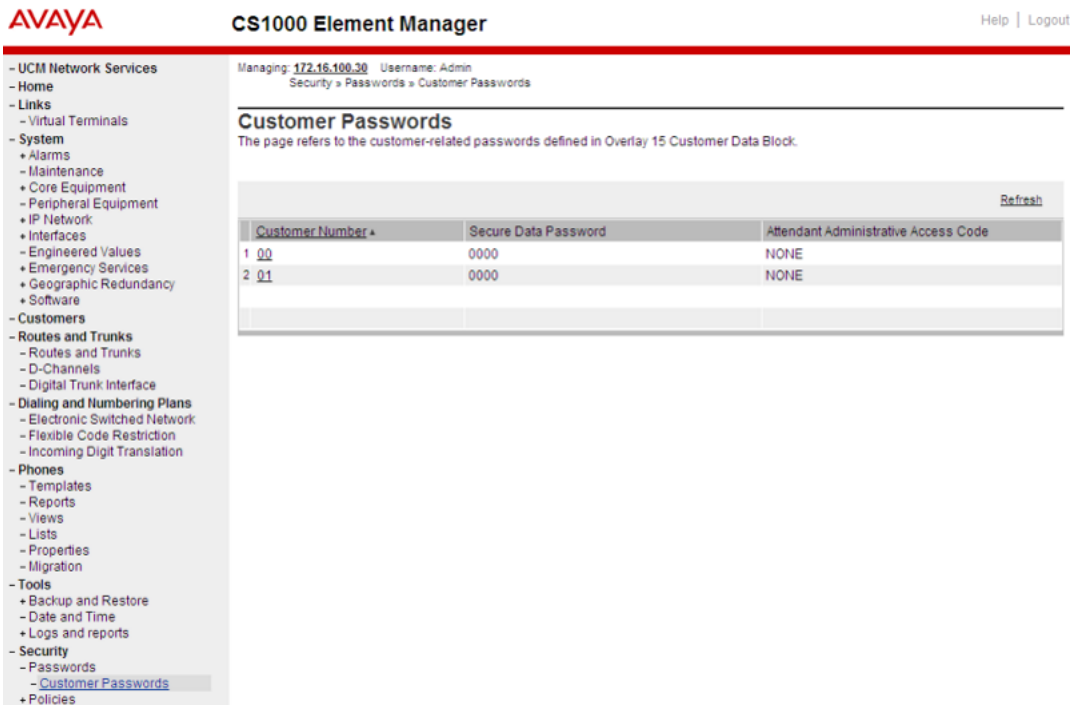
Customer passwords

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

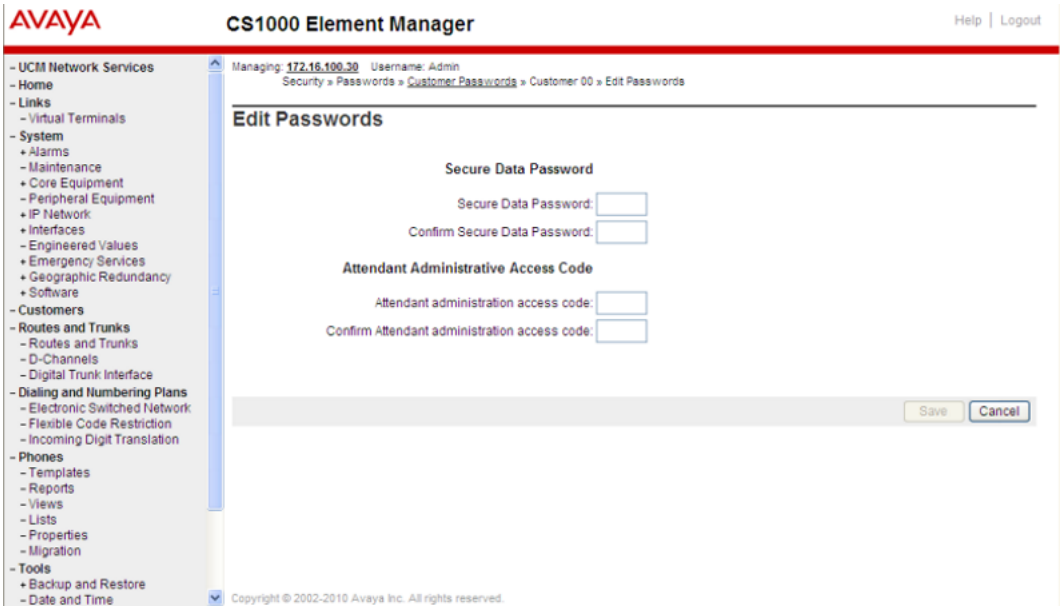
Use the following procedure to assign or change the Secure Data Password or Attendant Administrative Access Code.

Assigning or changing customer passwords

1. Log on to Element Manager using a System password level 2 account.
2. Click Security > Passwords > Customer Passwords . The Customer Passwords page appears.



3. Click a Customer Number. The Edit Passwords page appears.



4. Type the new secure data password in the **Secure Data Password**: field, and in the **Confirm Secure Data Password**: field.
5. Type the new secure data password in the **Attendant administration access code**: field, and in the **Confirm Attendant administration access code**: field.
6. Click **Save**.

   The Customer Passwords page appears.

View all user accounts

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Viewing account information by using LD 22

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 22 `REQ` prompt, enter **`prt`**.
3. At the LD 22 `TYPE` prompt, enter **`pwd`**.

   Details of all accounts appear.

Table 39: Example output from the PRT PWD command on page 201 shows an example of the output from the PRT PWD command.

Table 39: 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 AVAYA2 **INSECURE**
TYPE PWD2
USER_NAME AVAYA1 **INSECURE**
TYPE PWD1
USER_NAME LAPW1 **INSECURE**
TYPE LAPW)

OVLA     001     002     003     004     005     006     007     008     009     010
         011     012     013     014     015     016     017     018     019     020
         021     022     023     024     025     026     027     028     029     030
         031     032     033     034     035     036     037     038     039     040
         041     042     043     044     045     046     047     048     049     050
         051     052     053     054     055     056     057     058     029     060
         061     062     063     064     065     066     067     068     069     070
         071     073     073     074     075     076     077     078     079     080
         081     082     083     084     085     086     087     088     089     090
         091     092     093     094     095     096     097     098     099     117
         135     137     143

CUST
HOST NO
MAT NO
OPT PSCA RBBD CFPA LLCD PROD LOSD FORCD MOND
USER_NAME LAPW3 **INSECURE**
TYPE LAPW_OVL
OVLA 017 022
CUST
HOST NO
MAT NO
OPT PSCA RDBD DFPA LLCD PROD LOSE FORCD MOND
USER_NAME SBA2
PWTP SBA
LEVL ADMN
CUST
OPT FEAD NAMA TADD TOLD DTD TRKD INSD
```

User and password management using overlays

Use the information in this section to manage users, passwords, and privileges using LD 17 and LD 22.

User management

Use the procedures in this section to create, configure, and delete users.

Add a user

Use the following procedure to add a new PWD1 or PWD2 user.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Adding a user other than LAPW by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 REQ prompt, enter **CHG**.
3. At the LD 17 CHG prompt, enter **PWD**.
4. Bypass subsequent prompts (that deal with password settings, described later in this chapter) by pressing Enter at each one, until you reach the ACCOUNT_REQ prompt.
5. At the ACCOUNT_REQ prompt, enter **NEW** to create a new user.
6. At the PWD_TYPE prompt, enter **<account type>**.
7. At the LD 17 USER_NAME prompt, enter the user name to add or edit.
8. At the LD 17 PASSWORD prompt, enter the new password for the user, and reenter it at the CONFIRM prompt.
9. For PWD2 users, at the LD 17 ACCT prompt, enter either:

   YES to enable account management privileges for the new user,

   OR

   NO to disable account management privileges for the new user.
10. At the LD 17 PDT prompt, enter either: **PDT1** to grant the user access to PDT level one,

    OR

    PDT2 to grant the user access to PDT level two.

Table 40: Variable definitions

Variable	Value
<account type>	The type of account to create.

Table 41: Job aid: Restrictions on LAPW user names and passwords

Each LAPW user name can be up to 11 alphanumeric characters.
For LAPW SBA type users, the password must be 4-16 nonsequential numeric characters, and must consist of the digits 0-9 only.

The sequence of prompts for LD 17 is shown in Table 42: Job aid: LD 17 user and password prompts on page 203.

Table 42: 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 49: Job aid: Password restrictions on page 210.
NEW_PASSWORD	a...a	New password. For password requirements, see Table 49: Job aid: Password restrictions on page 210.
CONFIRM	a...a	Confirm the new password
ACCT	(NO) YES	Administer accounts. This prompt appears only when you add or modify Level 2 (PWD2) users.
PDT	(NO) PDT1, PDT2	PDT Access. This prompt appears only when you add or modify LAPW, Level 1 (PWD1) and Level 2 (PWD2) users.
OVLA	xx xx ... xx	Overlays Allowed

Table continues…

Prompt	Response	Comment
LEVL	aaaa	Access Level for Set Based Administration password, where; aaaa = (INST) or ADMN
CUST	aaa	Customer to be accessible by way of PWnn
TEN	xx	Tenant number (1–151)
HOST	(NO) YES	Enable HOST mode Log In for password PWnn
MAT	(NO) YES	Enable MAT Log In for password PWnn
OPT	a...a	Options for password PWnn
PDT	xxxx	PDT1 or PDT2

Note:

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

Add an LAPW user

Use the Limited Access to Overlays feature to create Limited Access Passwords (LAPW). LAPW users can access only the overlays you specify. You can define LAPW users that have regular access to specific overlays or that have Print Only capability, and you can use LAPW Audit Trail to track access to the system by LAPW users. The LAPW Audit Trail stores logon time, name, and password, and provides a time stamp indicating when the user logged out.

Use the procedures in this section to add and configure LAPW users. For more information about the prompts and options in LD 17, see *Avaya Software Input Output Administration, NN43001-611*.

Use the following procedures to create an LAPW user with Limited Access to Overlays type access:

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Adding an LAPW (Overlay) user by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 `REQ` prompt, enter **`CHG`**.
3. At the LD 17 `TYPE` prompt, enter **`PWD`**.
4. Bypass subsequent prompts by pressing `Enter` at each one.
5. At the LD 17 `ACCOUNT_REQ` prompt, enter **`NEW`** to add a new user.
6. At the LD 17 `PWD_TYPE` prompt, enter **`LAPW`**.
7. At the LD 17 `PWTP` prompt, enter **`OVLY`** to create an LAPW user that has Overlay Password Access.
8. At the LD 17 `USER_NAME` prompt, enter the user name to add or edit. SeeTable 45: Job aid: Restrictions on LAPW user names and passwords on page 206 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 49: Job aid: Password restrictions on page 210 for information about the restrictions on passwords.

10. At the LD 17 `OVLA` prompt, enter the overlays the new user can access.
11. At the LD 17 `CUST` prompt: press `Enter` to give the user access to all customer records, OR enter **<customer num>** , and then enter **TEN <tenant num>**, to specify the customers the user can access.
12. At the LD 17 `HOST` prompt, enter either: **YES** to enable HOST mode Log On for password PWnn, OR **NO** to disable HOST mode Log On for password PWnn.
13. At the LD 17 `MAT` prompt, enter either: **YES** to enable MAT Log On for password PWnn, OR **NO** to disable MAT Log On for password PWnn. If this option is enabled, MAT 5.0 users can remotely log on and perform Alarm Management and Maintenance operations through a graphical interface.
14. At the LD 17 `MAT_READ_ONLY` prompt, enter **YES** to grant MAT write access for password PWnn, OR **NO** to deny MAT write access for password PWnn. Read-only users cannot clear or acknowledge alarms, and can use status commands only.
15. At the LD 17 `OPT` prompt, enter **<options>**.
16. At the LD 17 `PDT` prompt, enter either:**PDT1** to grant the user access to PDT level one, OR **PDT2** to grant the user access to PDT level two.

Table 43: Variable definitions

Variable	Value
<customer num>	The customer number.
<options>	The password options permitted for password PWnn.
<tenant num>	The tenant number.

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

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

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 `REQ` prompt, enter **CHG**.
3. At the LD 17 `TYPE` prompt, enter **PWD**.
4. Bypass subsequent prompts by pressing `Enter` at each one.
5. At the LD 17 `ACCOUNT_REQ` prompt, enter **NEW** to add a new user.
6. At the LD 17 `PWD_TYPE` prompt, enter **LAPW**.
7. At the LD 17 `PWTP` prompt, enter **SBA** to create an LAPW user that has Set Based Access.
8. At the LD 17 `USER_NAME` prompt, enter the user name to add or edit. See Table 45: Job aid: Restrictions on LAPW user names and passwords on page 206 for information about the restrictions on LAPW user names.
9. At the LD 17 `PASSWORD` prompt, enter the new password for the user, and reenter it at the `CONFIRM` prompt. For LAPW SBA type users, the password must be 4-16 numeric characters, and must consist of the digits 0-9 only.

10. At the LD 17 `LEVL` prompt, enter either: **`INST`** to configure the access level of the user to be Installer, OR **`ADMN`** to configure the access level of the user to be Administrator.
11. At the LD 17 `CUST` prompt: press `Enter` to give the user access to all customer records, OR enter **`<customer num>`** , and then enter **`TEN <tenant num>`**, to specify the customers the user can access.
12. At the LD 17 `OPT` prompt, enter **`<options>`**.

Table 44: Variable definitions

Variable	Value
<customer num>	The customer number.
<options>	The password options permitted for password PWnn.
<tenant num>	The tenant number.

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

Table 45: Job aid: Restrictions on LAPW user names and passwords

Each LAPW user name can be up to 11 alphanumeric characters.
For LAPW SBA type users, the password must be 4-16 nonsequential numeric characters, and must consist of the digits 0-9 only.

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

Delete a user

Use the following procedure to remove a user.

Deleting a user by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 `REQ` prompt, enter **`CHG`**.
3. At the LD 17 `CHG` prompt, enter **`PWD`**.
4. Bypass subsequent prompts by pressing `Enter` at each one, until you reach the `ACCOUNT_REQ` prompt.
5. At the `ACCOUNT_REQ` prompt, enter **`OUT`** to delete a user.
6. At the `USER_NAME` prompt, enter the name of the user to delete.

   The following message appears: `WARNING: THIS ACCOUNT WILL BE DELETED OK? (Y/N)`
7. Enter **`Y`** to delete the user.

Check for Insecure passwords

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Checking for insecure passwords using LD 22

1. At the LD 22 REQ prompt, enter **PRT**.
2. At the LD 22 TYPE prompt, enter **IPWD**.

Table 46: IPWD output on page 207 shows an example of the output form the PRT IPWD command.

Table 46: IPWD output

```
PWD
User_Name AVAYA2 **INSECURE**
TYPE PWD2
User_Name AVAYA1 **INSECURE**
TYPE PWD1
USER_NAME LAPW1 **INSECURE**
TYPE LAPW_OVL
USER_NAME LAP3  **EXPIRED**
TYPE LAPW3_OVL
```

Configure LAPW Audit Trail using overlays

The Audit Trail for Limited Access Password (LAPW) stores logon time, name, and password, and includes time stamps that indicate when users logged out.

Use the following procedure to enable or disable Audit Trail and configure the size of the Audit Trail file.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Configuring the LAPW Audit Trail by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 REQ prompt, enter **CHG**.
3. At the LD 17 TYPE prompt, enter **PWD**.

   You can bypass any of the subsequent prompts by pressing Enter. For more information about the sequence of prompts for LD 17, see Table 42: Job aid: LD 17 user and password prompts on page 203.
4. At the LD 17 AUDT prompt, enter either: **YES** to enable the Audit Trail, OR **NO** to disable the Audit Trail.

5. At the LD 17 SIZE prompt, enter **<SIZE>**.

   After the Audit Trail file becomes full, no more information can be stored in it. Avaya recommends periodically backing up the file and deleting the contents.

6. Bypass subsequent prompts by pressing Enter at each one.

Table 47: Variable definitions

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

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

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

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 22 REQ prompt, enter **PRT**.
3. At the LD 22 TYPE prompt, enter **AUDT** to view the Audit Trail.

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 42: Job aid: LD 17 user and password prompts on page 203.

To view LAPW prompts, you must equip package 164 LAPW Limited Access to Overlays. LAPW users can change their passwords by entering the current password at prompt LPWD and entering the new password at the NLPW prompt.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Changing a password by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has that has ACCT=YES.
2. At the LD 17 REQ prompt, enter **CHG**.
3. At the LD 17 CHG prompt, enter **PWD**.
4. Bypass subsequent prompts by pressing Enter at each one.
5. At the ACCOUNT_REQ prompt, enter **CHG**.
6. At the USER_NAME prompt, enter the user name to change the password.
7. At the NEW_PASSWORD prompt, enter the new password, and reenter it at the CONFIRM prompt.

You can use the following procedure to change the password for your PDT user name using the PDT shell command line interface (CLI).

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Changing your PDT password by using the CLI

1. Log on to the Call Server CLI using an account that has PDT privilege.
2. Access the PDT prompt by holding down the `ctrl` key, and typing `pdt`. The PDT prompt appears.
3. Enter the command `passwd`.
4. Enter your existing password.
5. Enter the new password. The new password must be different from the current password.
6. Reenter the new password. A confirmation message appears.
7. To exit PDT mode, type `exit`, and press `Enter` twice.

These changes are distributed to all Voice Gateway Media Card, Gateway Controller, 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 on page 275.

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 on page 46. For recommendations about what password settings to use, see Recommended password management practices on page 50.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Important:

Avaya 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.

Configuring password settings by using LD 17

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 17 `REQ` prompt, enter **`CHG`**.
3. At the LD 17 `CHG` prompt, enter **`PWD`**.

   You can bypass any of the following prompts by pressing `Enter`. For more information about the sequence of prompts for LD 17, see Table 42: Job aid: LD 17 user and password prompts on page 203.
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 49: Job aid: Password restrictions on page 210.

5. At the LD 17 `FPC` prompt, enter **`YES`** to enable Force Password Change. Configuring FPC to YES closes LD 17; to continue configuring password settings in LD 17, repeat steps 2-4, enter NO at the FPC prompt, and then proceed to step 6.

   The FPC = YES value is not retained in the database and must be configured to YES each time you want to force a change.
6. At the LD 17 `LOUT` prompt, enter **<LOUT>** to enable Inactive Session Timeout.
7. At the LD 17 `FLTH` prompt, enter **<FLTH>** to enable Failed Log in Threshold.
8. At the LD 17 `LOCK` prompt, enter **<LOCK>** to configure the Lockout time.
9. At the LD 17 `FLTA` prompt, enter **`YES`** to enable Failed Log In Threshold Alarm.
10. At the LD 17 `AUDT` prompt, enter **`YES`** to enable Audit Trail for password usage. The `SIZE` prompt appears.
11. At the LD 17 `SIZE` prompt, enter **<SIZE>** to configure the word size of Audit Trail buffer.
12. At the LD 17 `LLID` prompt, enter **`YES`** to enable Last Login Identification.
13. Bypass subsequent prompts by pressing `Enter` at each one.

Table 48: Variable definitions

Variable	Value
<SIZE>	The word size for the Audit Trail file, in the range of 50–1500. The default value is 50.
<FLTH>	The number (in the range 0–9) of times a user can successively fail to log on before their account is locked out.
<LOCK>	The number (in the range 0–270) of minutes an account remains locked after the Failed Log in Threshold is reached.
<LOUT>	The number (in the range 1–1440) of minutes of inactivity before a session ends automatically.

Table 49: 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)

Table continues…

- have five or more consecutive alphabetic characters

Password reset

Use the procedures in this section to reset passwords on the Call Server, or on other devices. To use these procedures, you must disable UCM central authentication and reset the locally-authenticated Communication Server 1000 Call Server accounts (admin1, admin2, pdt2). You must have the applicable software install media (floppy disk or flash card) on hand, and must insert it only when prompted to do so during the password reset procedure.

Use the following procedure to reset an individual password on the Call Server, and lock out all other accounts. To protect against unauthorized use, Avaya 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.

Resetting Call Server passwords by using the CLI

1. Log on to the Call Server CLI using an account that has PDT privilege.
2. Access the PDT prompt by holding down the **ctrl** key, and typing **pdt**. The PDT prompt appears.
3. Instead of entering a user name, enter **resetPWD**.

   The Password Reset Mechanism is initiated, and the following message appears:

   ```
   PDT login on /tyCo/0 Username: resetPWD
   ********************************************** * WARNING: All
   attempts to use the Password Reset Mechanism * * are logged. In
   order to proceed, you will need * * physical access to the Call
   Server. * ********************************************** If you do
   not wish to proceed, enter the word QUIT, otherwise enter the PWD2/
   Admin2 userID: SEC026 Password override mechanism was used to gain
   access to the switch
   ```

4. Enter either: **QUIT** to exit without resetting any passwords, OR **<user name>**.

   If the user name you enter exists on the system, it is the target of the password reset. If the user name you enter does not exist on the system, a new PWD2 level account is created.
5. When prompted, insert the install media in the disk drive or PC Card slot. You must complete this step within 60 seconds, or the Password Reset Mechanism cancels.
6. Press Enter.
7. Enter the new PWD2 password.
8. Reenter the new PWD2 password.
9. To exit PDT mode, type **exit**, and press Enter twice.
10. Remove the install media from the drive.

    The system changes the password for the account (or creates a new account and assigns it the new password) and locks out all other accounts. The system marks the new password as

expired, so the user must change it on their next log on. If the account is locked because the user exceeded the Failed Log in Threshold, the system unlocks it.

These changes are distributed the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see Force an EDD using overlays on page 275.

Table 50: Variable definitions

Variable	Value
<user name>	A PWD2 level user name.

Use the following procedure to reset the password on an MGC or CP MG card.

Resetting MGC and CP MG passwords by using the CLI

1. Use a direct serial connection to connect to the CLI of the Gateway Controller.
2. At the log on prompt, enter the reset password command: **`Username: resetPWD`**. The following output appears: `********** * WARNING: All attempts to use the Password Reset Mechanism * * are logged. In order to proceed, you will need * * physical access to the Call Server. * ********** If you do not wish to proceed, enter the word QUIT, otherwise enter the PDW2/Admin2 userID:`
3. Enter the user name for which you want to reset the password. The following output appears: `You have 60 seconds to push the reset faceplate button`
4. Press the reset button on the Gateway Controller faceplate. The following output appears: `You have 60 seconds to press ENTER:`
5. Press `Enter`. The following output appears: `Enter new password: .`
6. Enter the new password. The following prompt appears: `Reenter new password:`
7. Reenter the new password.

Password reset for other devices

For information about password reset procedures on other devices, see Table 51: Password reset for Linux base elements on page 212.

Important:

To reset the password on Voice Gateway Media Cards, ensure that the card is properly registered to the Call Server and then reboot the card. This forces synchronization of the user names and passwords with the Call Server user names and passwords.

Table 51: Password reset for Linux base elements

Device or application	For more information about the reset procedure, see:

Table continues…

CallPilot mailbox	*Avaya CallPilot Manager Set Up and Operation Guide, NN40090-300*
Contact center user	*Avaya Contact Center Manager Server Installation and Maintenance, 297-2183-925* and *Avaya Contact Center Manager Server Installation and Maintenance Guide for the Co-resident Server, 297-2183-925*
Hospitality Integrated Voice Services	*Avaya Hospitality Integrated Voice Services Fundamentals, NN43001-559*
Integrated Call Director	*Avaya Integrated Call Director Service Implementation Fundamentals, NN43001-561*
IP Line	*Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
Signaling Server	*Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*

If Service Provider certificates are installed on an IP Phone, you can remove them by resetting the phone security policies, and other values, to factory defaults. For more information, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Multi-user login configuration using overlays

For normal system management access for multi-user login configurations, use Element Manager, UCM Central Deployment Manager and Patching Manager, and web services API in preference to using OAM CLI access.

Enable Multi-user login to permit up to five users to simultaneously log on to a system. Each user can load a different overlay (LD), and a sixth overlay (virtual midnight or background) can also run. If a user tries to load an overlay that another user is already using, an error message appears. This feature supports only:

- telephone administration
- maintenance
- midnight routines
- background routines
- attendant administration

Multi-user login supports a maximum of five users; if a sixth user attempts to log in, the system blocks the attempt. Use the monitor command to monitor the input/output activities on another local or remote terminal.

You can configure Multi-user login using LD 17, and view information about Multi-user login configuration using LD 22. For more information, see *Avaya System Management Reference, NN43001-600*.

Single Terminal Access configuration using overlays

Avaya does not recommend the use of the Single Terminal Access (STA) feature. If you want to provide remote access to multiple SDI ports on the Communication Server 1000 system elements

and auxiliary servers and devices, Avaya recommends using an optional IP terminal server and to obtain technical support for configuring the terminal server from the terminal server equipment vendor.

uses Multipurpose Serial Data Link (MSDL), which reduces the number of physical devices you must have for administration and maintenance. For remote access over IP networks, you can configure a terminal server to provide a cost-effective method of switching between EIA232 serial port devices. When a user switches from one system to another, a mechanism for ending the original session is provided in the STA application through a configurable logoff sequence. This logoff sequence is specified in the database with each STA port, and is automatically sent to the destination system.

To protect against unauthorized access, the following rules apply:

- Users cannot leave the system without logging off, preventing users from leaving a session open in the background. If the logoff sequence is not configured correctly, the user can leave a program open in the background, which can lead to unauthorized access.
- If the modem connection is terminated, the STA master terminal uses the configured logoff sequences to automatically exit from the active and existing background sessions.
- A password is required before the user can enter **NEW** or **CHANGE** to configure an STA port. This process is designed to protect the STA port from unauthorized alteration.

You can configure STA using LD 17, and view information about STA configuration using LD 22. For more information, see *Avaya 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 *Avaya 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 *Avaya System Management Reference, NN43001-600*.

Note:

The dsameuser account is a UCM system login account used for several UCM operations. These operations are logged and may appear in the History File.

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 52: User administration commands on page 215.

Table 52: User administration commands

Command	Description
adminUserPasswordChange [userID]	To change a password (any user can change their own password, but only users that have Level 2 [PWD2] privilege can change the password of another user). Where `userID` is the name of the user account to change.
adminUserCreate [userID]	To create an account (requires Level 2 (PWD2) privilege). Where `userID` is the name of the user account to create.
adminUserDelete [userID]	To delete an account (requires Level 2 (PWD2) privilege). Where `userID` is the name of the user account to delete.
adminAccountShow	To display all configured accounts on the system (requires Level 2 (PWD2) privilege).

User and password management using Element Manager

Use the procedures in this section to manage users, change passwords, and configure access restrictions using Element Manager. Users without the Administer Accounts privilege can change their own password only.

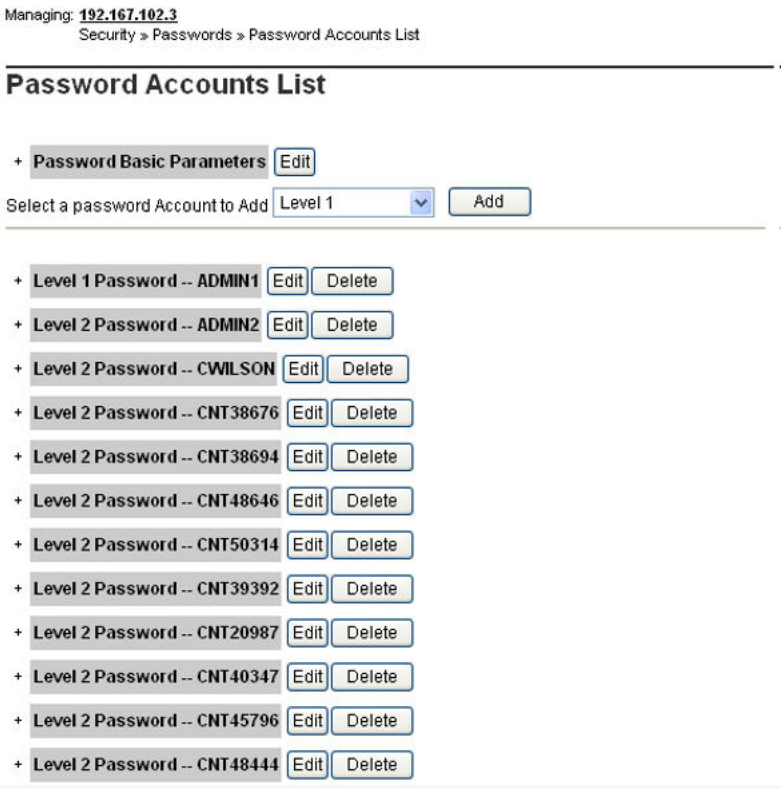
Add a user

Use the following two procedures to add user accounts.

Adding a user other than LAPW by using Element Manager

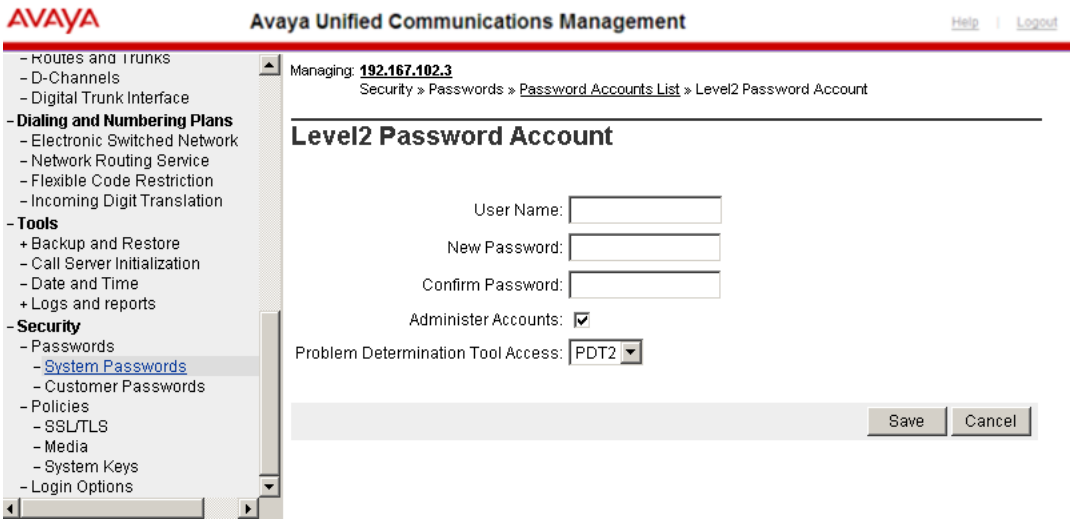
1. Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2. Click Security > Passwords > System Passwords.

   The Password Accounts List page appears.



3. From the **Select a password Account to Add** list, select one of the listed account types. For more information about the account types available, see System accounts on page 43.
4. Click **Add**.

   The Password Account page appears. The page varies slightly depending on what type of account you selected.

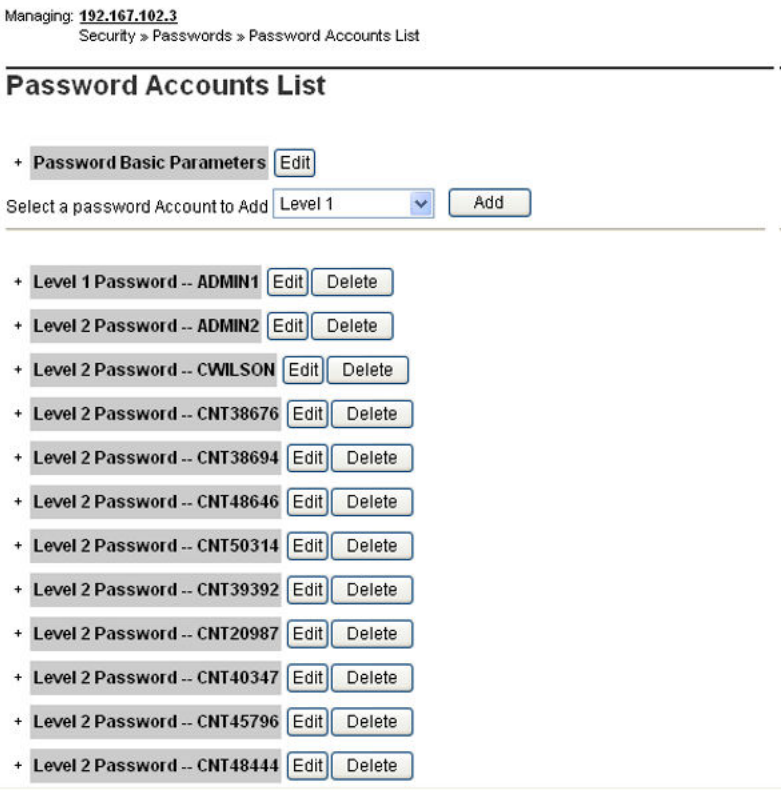


5. Enter the user name in the **User name** field, and the password in the **New password** and **Confirm password** fields.
6. Choose from one or more of the following options, depending on the type of account you are adding:
    a. If you are adding a Level 1 or Level 2 account, and want to give the user PDT access, make a selection in the **Problem Determination Tools Access** list.
    b. If you are adding a Level 2 account, select or clear the **Administer Accounts** check box.
7. Click **Save** to save the new user, and return to the Password Accounts List page.

Adding an LAPW user by using Element Manager

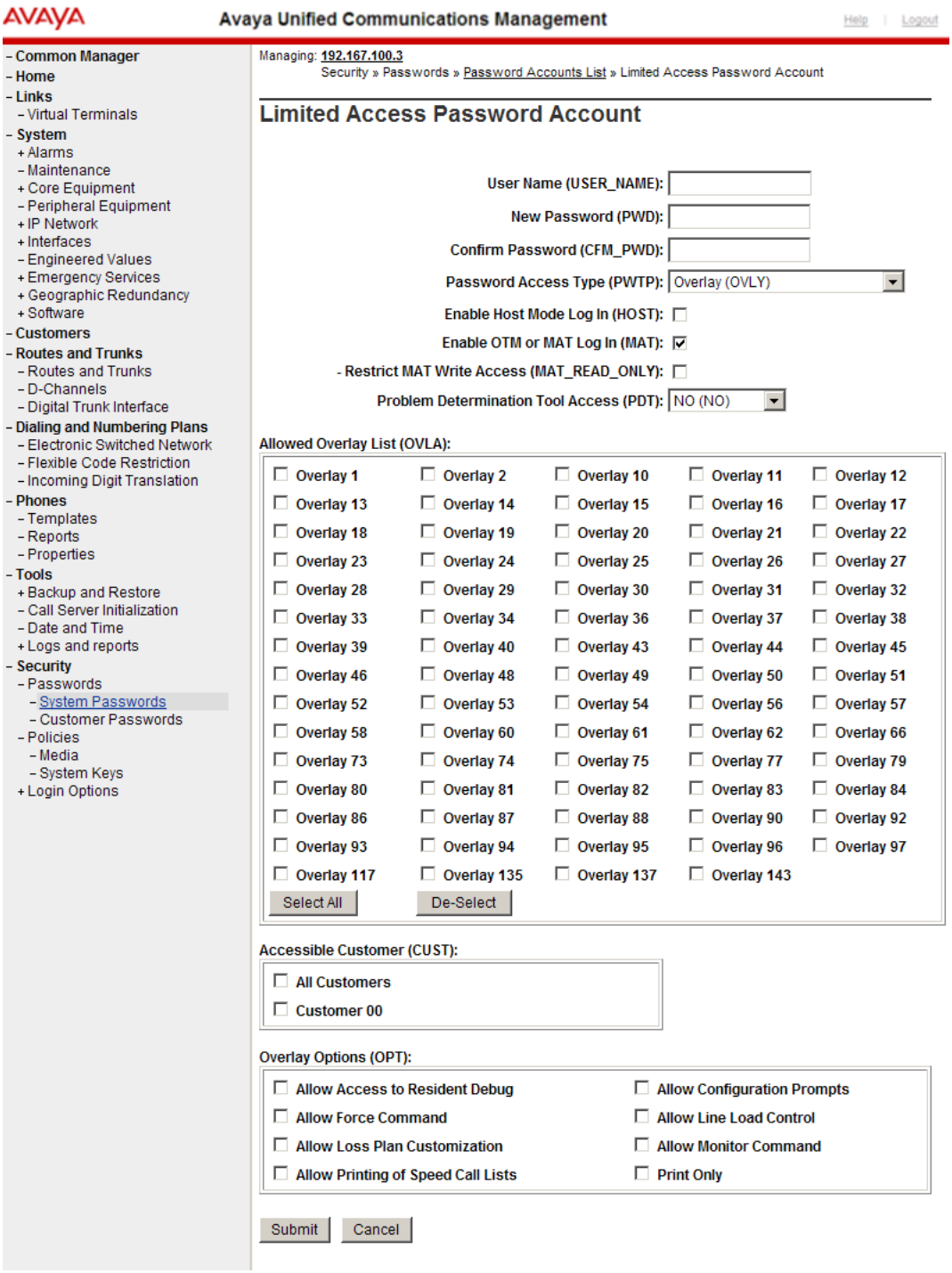
1. Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2. Click Security > Passwords > System Passwords.

    The Password Accounts List page appears.



3. From the **Select a password Account to Add** list, select **Limited Access**. For more information about the account types available, see System accounts on page 43.
4. Click **Add**.

   The Limited Access Password Account page appears.



5. Type the new user name in the **User name** field.
6. Type the password for the new user in the **New password** and **Confirm password** fields.
7. In the **Password access type** list, choose either **Overlay (OVLY)** or **Set Based Administration (SBA)**.
8. Select or clear **Enable host mode log in**.

9. Select or clear **Enable OTM or MAT Log In (MAT_READ_ONLY):**
10. Select or clear **Restrict MAT Write Access (MAT_READ_ONLY):**
11. In the **Problem Determination Tool Access (PDT)** list, choose one of **NO**, **PDT1** or **PDT2**
12. Select or clear the various overlays in the **Allowed Overlay List (OVLA)** list. You can use the **Select All** and **De-Select** buttons to select or clear all of the overlays in a single step.
13. Select or clear the various customers in the **Accessible Customer (CUST)** list.
14. Select or clear the various options in the **Overlay Options (OPT)** list.
15. Click **Submit** to save the new user, and return to the Password Accounts List page.

Edit an existing user

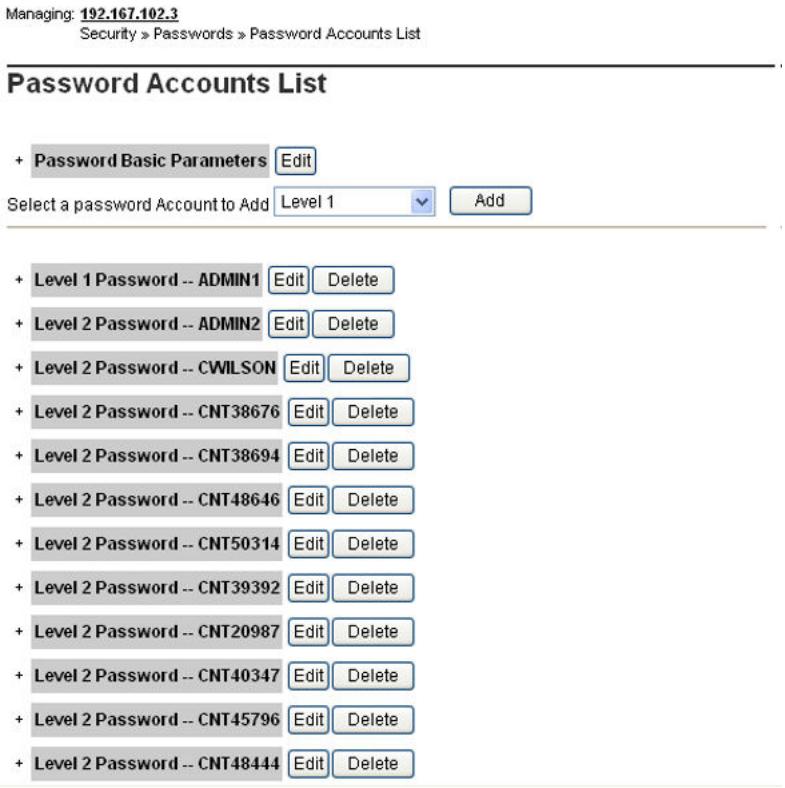
Use the following procedure to edit user accounts, including changing a user's password.

To change passwords for Level 1 and Level 2 accounts, you must log on using an account that has Level 2 access.

Editing an existing user by using Element Manager

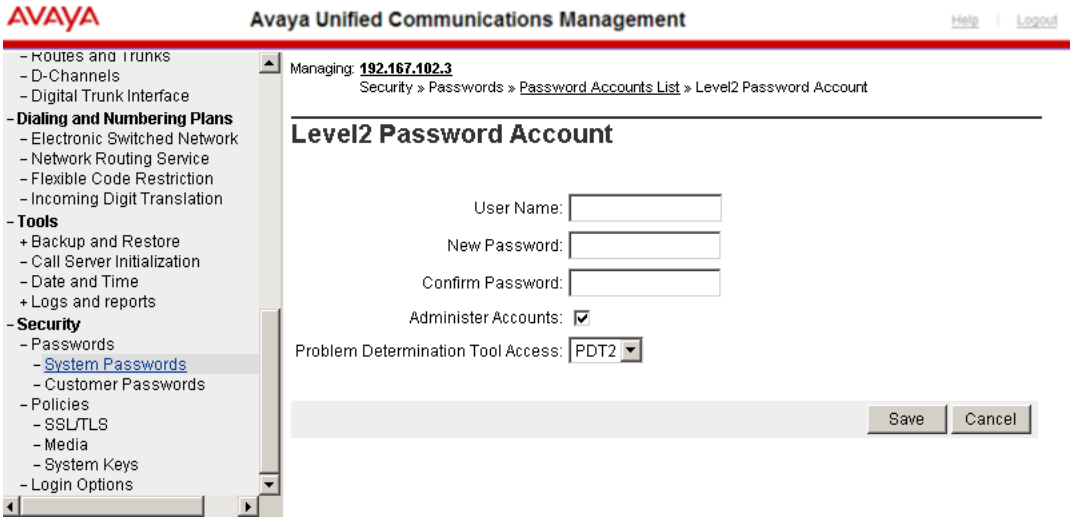
1. Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2. Click Security > Passwords > System Passwords.

   The Password Accounts List page appears.



3. Next to the account you want to modify, click **Edit**.

   The Password Account page appears.



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

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

Synchronize a changed password

The Synchronize a changed password option is selected by default and prompts an EDD in the Call Server after the passwords are changed successfully. You must perform an EDD, or wait for the next scheduled EDD, to synchronize the password across the servers linked to the Call Server.

Manage passwords for stand-alone Signaling Server using NRS

Level 2 (PWD2) users manage accounts and passwords on the stand-alone Signaling Server running Network Routing Service (NRS).

Use the following procedure to access the PDT prompt on the stand-alone NRS. At the PDT prompt, you can execute OAM commands, as well as Avaya debug commands, and user and password management commands for the stand-alone NRS. For more information about user and password management commands available at the PDT prompt on the stand-alone NRS, see Table 53: Job aid: user and password management commands on the stand-alone NRS on page 222.

Accessing the PDT prompt on stand-alone NRS

1. Log on to the NRS OAM shell using an account having admin privilege.
2. Access the PDT prompt by holding down the **ctrl** key, and typing **pdt**. The PDT prompt appears.

Table 53: Job aid: user and password management commands on the stand-alone NRS

Command	Description
adminUserPasswordChange [userID]	Use this command to give users the ability to change their own password, or to give a Level 2 (PWD2) user the ability to change any user password specified in the userID field. Requires Level 2 (PWD2) access.
adminUserCreate [userID]	Use this command to create an account specified in the userID field. Requires Level 2 (PWD2) access.
adminUserDelete [userID]	Use this command to delete an account specified in the userID field. Requires Level 2 (PWD2) access.
adminAccountShow	Use this command to display all configured accounts on the system. Requires Level 2 (PWD2) access.

Change an expired password

If you log on using an expired password, you are directed immediately to the System Password Change facility of Element Manager. Enter a new password (and reenter it to conform the spelling), as shown in Figure 17: System password change on page 222.

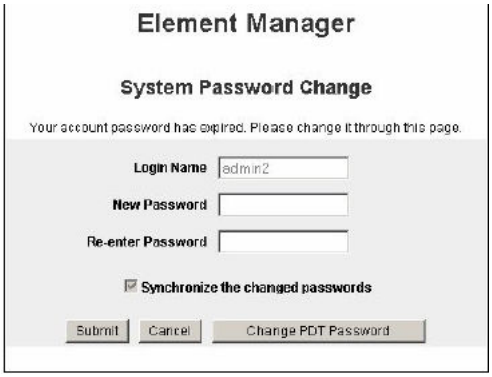


Figure 17: System password change

Edit global password settings

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

Table 54: Job aid: password options

Password option	Effect
Force Password Change (FPC)	Prevents users from continuing to use the system default passwords.
Failed Log In Threshold	Controls the number of times a user can fail to log on before the port they are using is locked. To override a lockout, manually restart the system.

Table continues…

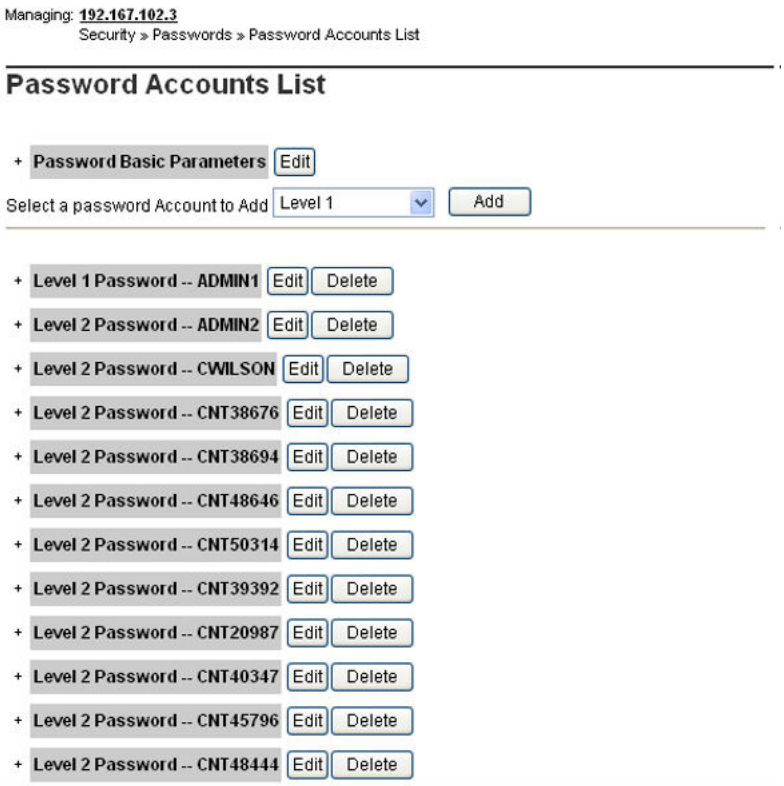
Password option	Effect
Failed Log In Threshold Alarm	Sets an alarm whenever the Failed Log in Threshold is exceeded.
Port Lockout Time After Failed Log in	Controls the length of time the port is locked after the Failed Log In Threshold value is reached.
Password Complexity Check	Tests user passwords to verify that they are difficult to guess.
Audit Trail for Password Usage	Prevents the reuse of a password.
Word Size of Audit Trail buffer	The size for the Audit Trail file, in the range of 50–1500. The default value is 50.
Last Log In Identification	Keeps track of the last user who logged on.
Inactivity Timeout	Ends a logon session after a period of inactivity.

For more information about the features described in this section, see Global password settings on page 46.

Editing global password settings by using Element Manager

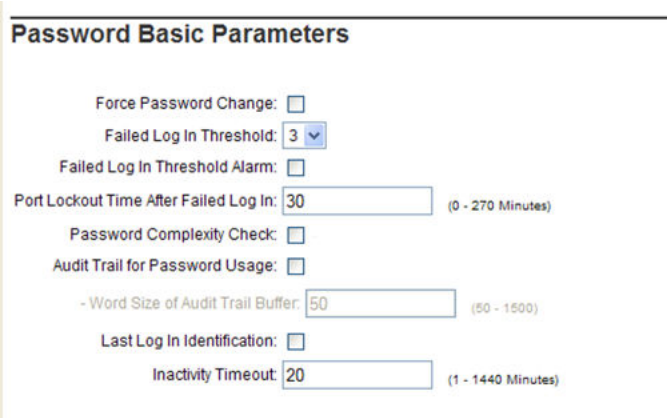
1. Log on to Element Manager using a System password level 2 account that has Administer Accounts privilege.
2. Click Security > Passwords > System Passwords.

   The Password Accounts List page appears.



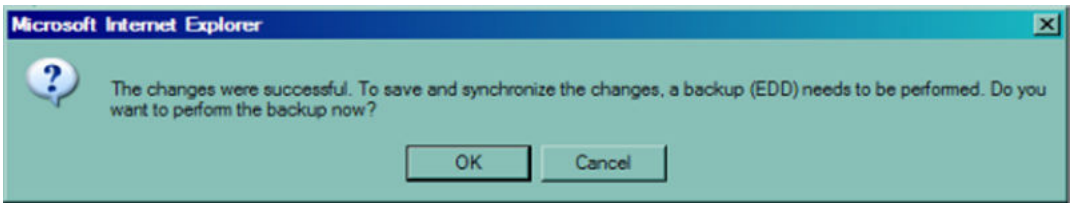
3. Next to **Password Basic Parameters**, click **Edit**.

   The Password Basic Parameters page appears.



4. Edit any of the following parameters by selecting or clearing the check box, selecting from the list, or entering a value:
   - Force Password Change
   - Failed Log in Threshold
   - Failed Log In Threshold Alarm
   - Port Lockout Time After Failed Log in
   - Password Complexity Check
   - Audit Trail for Password Usage
   - Word Size of Audit Trail buffer
   - Last Log In Identification
   - Inactivity Timeout
5. Click **Save** to save the changed password settings, and return to the Password Accounts List page.

   The following message appears:



6. Click **OK** to perform an EDD.

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 on page 222.

Chapter 11: 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 on page 225)
- switchroom security (see Switchroom security on page 226)
- network facilities security (see Network facilities security on page 226)

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.

Use passwords to limit access to the system communication ports.

Switchroom security

Ensure that the room where the switch is physically located is secure, otherwise unauthorized users can access all system resources. Unauthorized users can take actions such as turning off printer and CDR processors or removing cards from the system, which renders the system inoperable. Follow these security procedures to minimize this risk:

- Limit access to the switchroom to authorized personnel only.
- Require distributor and telephone company personnel to sign in and out and provide identification, if necessary.
- Control, document, and audit major changes to system configuration.
- Require personnel to sign out parts and equipment.
- Store printouts of system configurations and databases in a secure, locked area.
- Do not post passwords or Trunk Access Codes in the switchroom.
- Keep the switchroom and telephone equipment closets locked.

Network facilities security

Network security is just as important as switchroom security. For example, unsecured facilities can be accessed using a test terminal to place unauthorized calls without these calls being detected by the system and recorded by the CDR.

Follow these security procedures to minimize this risk of misuse:

- Secure the telephone company access point, individual distribution frame location, and the Main Distribution Frame (MDF).
- Avoid locating Intermediate Distribution Frames (IDF) in janitorial, electrical, and supply closets. Limit access when collocation is unavoidable.

- Document existing outside and inside cable plans and update these records as service changes are made.
- Where cable plan records do not exist, consider hiring an independent consultant to verify and document the cable plan.
- Maintain and document all moves and changes. Eliminate all out-of-service cross connects if not using the Automatic Set Relocation feature.
- Encase and lock building entry terminals and secure manholes.
- Avoid posting cable documentation in the IDF.
- Keep cable plant documentation in at least two separate secure locations.
- Verify terminal connections against cable plant and system records, and resolve all differences.
- Audit the entire system, ensuring that all cable, telephone company, telephone, and system records are accurate.
- Limit access to the ELAN using firewalls or appropriate data network configuration. Physical access and data network access to the ELAN is recommended to protect the system from attacks.

Add or remove elements from the UCM security domain

Use the commands in Table 55: Commands for adding or removing elements from the UCM security domain on page 227 to add or remove elements from the Unified Communications Management security domain.

Before issuing the commands to join the security domain, ensure that all elements are active and known to the Call Server.

Table 55: Commands for adding or removing elements from the UCM security domain

Command	Type	Preconditions	Description
`joinSecDomain`	OAM/PDT CLI	• PWD2 privilege • UCM security IP address • Username and password for a UCM administrator whose UCM role includes the Security Administrator	Establish mutual trust with the primary security server. **Note:** To use this command, you must first Telnet into the ELAN IP.
`leaveSecDomain`	OAM/PDT CLI	• PWD2 privilege • Member of UCM security domain	Remove the primary security server mutual trust information from the device.

Table continues…

Command	Type	Preconditions	Description
			Note: To use this command, you must first Telnet into the ELAN IP.
statSecDomain	OAM/PDT CLI	• PWD2 privilege • Member of UCM security domain	Display the primary security server IP address and fingerprint. **Note:** To use this command, you must first Telnet into the ELAN IP.
Register UCMSecurity CS	LD 117	• admin1 or admin2 privilege	Establish mutual trust with the primary security server for the Call Server. If the Call Server is already registered, it reregisters.
Register UCMSecurity Device [<ip_address>]	LD 117	• admin1 or admin2 privilege • username and password for a UCM administrator whose UCM role includes the Security Administrator Linux base element	Establish mutual trust with the primary security server for the element specified by <ip_address>, where <ip_address> is a VGMC or Gateway Controller registered to a Call Server belonging to the UCM security domain.
Register UCMSecurity System [Force]	LD 117	• admin1 or admin2 privilege • UCM security IP address • username and password for a UCM administrator whose UCM role includes the Security Administrator Linux Base element	All associated elements, such as Gateway Controllers and VGMCs, join the UCM security domain after prompting for user approval. (If the system is a redundant system, the inactive Call Server joins the security domain automatically.) Use FORCE to request all elements to register to the primary security server. Elements that are already registered will reregister.
Stat UCMSecurity info	LD 117	• An account with the NetworkAdministrator role assigned	Display the primary security server IP address and fingerprint.

Table continues…

Command	Type	Preconditions	Description
		• Member of UCM security domain	
Stat UCMSecurity System [Refresh]	LD 117	• No privilege requirement • Member of UCM security domain	Display all known CS 1000 elements (such as Gateway Controller, MC32, MC32S) and their current UCM security domain status as Registered or Unregistered. Use [Refresh] to refresh the list.
Unregister UCMSecurity CS	LD 117	• An account with the NetworkAdministrator role assigned	Remove the mutual trust information from the primary security server for the Call Server.
Unregister UCMSecurity Device [<ip_address>]	LD 117	• An account with the NetworkAdministrator role assigned	Remove the mutual trust information from the primary security server for the device specified by <ip_address>.
Unregister UCMSecurity System	LD 117	• An account with the NetworkAdministrator role assigned	Remove the mutual trust information from the primary security server for the Call Server and all of its associated Gateway Controllers and VGMCs.

Note:

When using the OAM/PDT CLI, you must telnet to the ELAN IP to access security-related commands.

Note:

When you reboot Media Gateway devices after upgrade (except for MC32S), log messages dsLOG003 tAccountTransfer and LOG003 tBannerTransfer display due to the account database and banner file transfer failing while the device waits to register with the UCM security domain.

Note:

PWD2 is the pre-membership system password. It does not exist after the system joins the security domain.

Note:

If /e/keys/known_host or /e/keys/<IP address>.pub files exist prior to the upgrade from 5.5, it is not possible to join the security domain via executing the command, reg ucm sys. Perform the following steps to join the security domain:

1. Remove the pub files manually.
2. Execute the command **unreg ucm sys**.

3. Execute the command **reg ucm sys force**.

VxWorks systems and devices

Note:

You need a CLI (telnet, rlogin or ssh) connection to use security domain registration commands.

VxWorks based systems and devices can join the Unified Communications Management security domain using the following modes:

- User mode (preferred)—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:
  - LD 117 command: **[REGISTER / UNREGISTER] UCMSECURITY SYSTEM**
- Manual mode—the joining and leaving of the Unified Communications Management security domain operation is performed on each individual Call Server, Gateway Controller and Voice Media Gateway Card using the following commands:
  - LD 117 command: **[REGISTER / UNREGISTER] UCMSECURITY DEVICE**
  - OAM/PDT/IPL commands: **joinSecDomain** or **leaveSecDomain**

Before issuing the commands to register to the security domain, ensure that all elements are active and known to the Call Server. Also, when upgrading a pre-Release 6.0 Communication Server 1000 system to Release 6.0 or higher, ensure that secure transfer (sFTP) is disabled before transferring loadware and registering all MGCs, VGMCs and MCs to the Call Server. You can then enable sFTP after successfully registering these devices to the Call Server and before registering them to the security domain.

Note:

If **REG UCM SYS** is executed after upgrade and data files were preserved during the upgrade, there is a possibility that old files are stored in /e/sdm and therefore no prompt for UCM IP is given. In this case, command **REG UCM SYS FORCE** must be used. For more information, see Add or remove elements from the UCM security domain on page 227.

Adding elements to the security domain when ISSS is enabled

Before adding a non-Linux element (such as Media Card and Gateway Controller) to a security domain where ISSS is enabled, do the following:

- Add a new manual IPsec target with the IP address as the ELAN IP address of the non-Linux element. Ensure that the **Enable IPsec** check box is not selected.
- Synchronize and activate the IPsec configuration using Graceful mode.

Note:

If ISSS is enabled in FULL mode and is hardened, you must enable FTP as it is disabled on the Call Server and Signaling Server during the hardening process (sFTP is used by default). FTP

is required for updating the loadware on the card, which enables it to register to the UCM security domain.

This process allows the non-Linux element to communicate with the Call Server or Element Manager without using IPsec so that any required updates can be applied to the element prior to registering with the security domain. The manual IPsec target is replaced with the correct automatic target when the element registers with UCM.

If you are replacing a non-Linux element (such as Media Card and Gateway Controller), instead of adding a new manual ISSS target you must disable IPsec for the appropriate automatic target in UCM. Do this as follows:

- Select the radio button beside the target being replaced and click **IPsec Not Required**.
- Synchronize and activate the IPsec configuration using Graceful mode.

To minimize the required steps during an upgrade or new installation, Avaya recommends that you register all (or most) elements before enabling ISSS.

Co-resident Call Server and Signaling Server systems

Co-resident systems can join the Unified Communications Management security domain using the following modes:

- User mode—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:
  - LD 117 command: **`[REGISTER / UNREGISTER] UCMSECURITY SYSTEM`**

This command can only be used to join the associated Gateway Controllers and Voice Gateway Media Cards to the security domain and not the Call Server itself. In the Co-resident Call Server and Signaling Server configuration, the Call Server is joined to the security domain with Linux base during installation.

Join a Co-resident Signaling Server to the UCM security domain using Base Manager

You can use Base Manager to join a Co-resident Signaling Server to the UCM security domain.

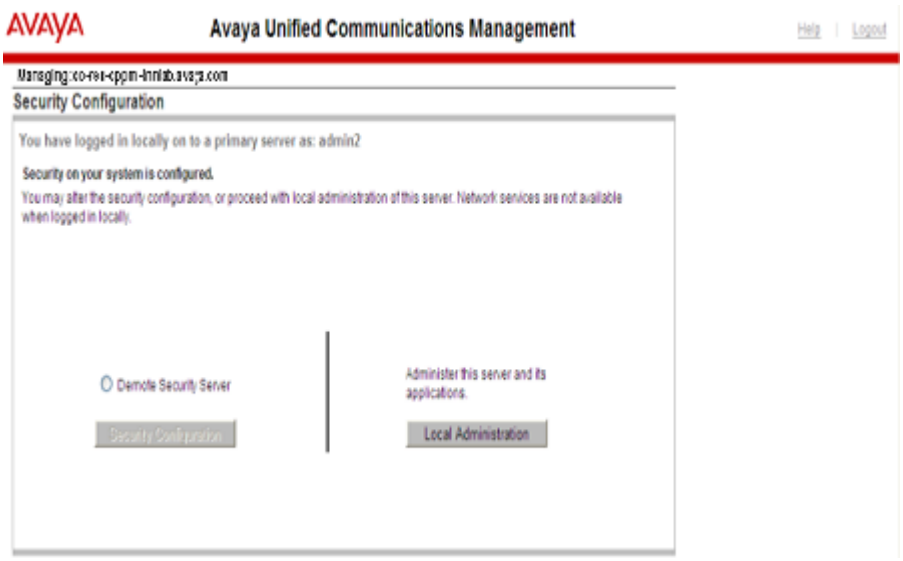
You must join the Signaling Servers to the UCM security domain in the following order:

- Primary server
- Backup server
- Member server

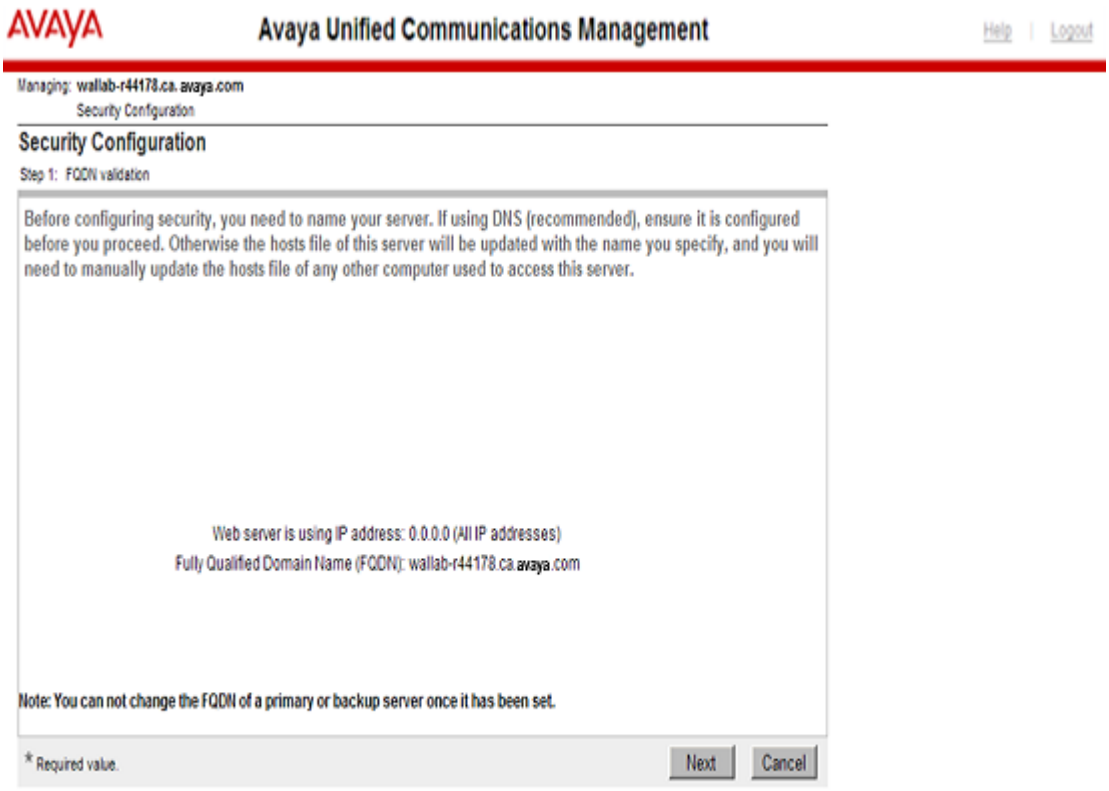
For the procedure to login and access the Base Manager application, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Joining a Primary security server to the UCM security domain using Base Manager

1. From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**.

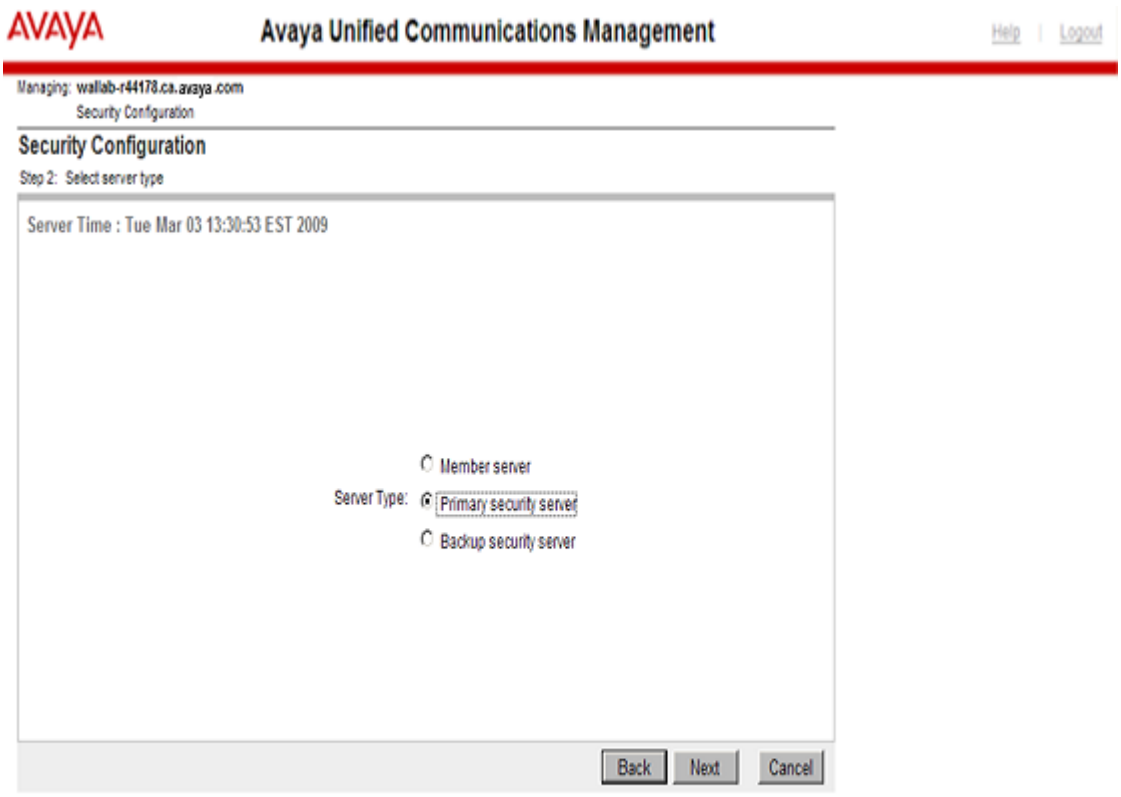


The **Step 1: FQDN validation** page appears.



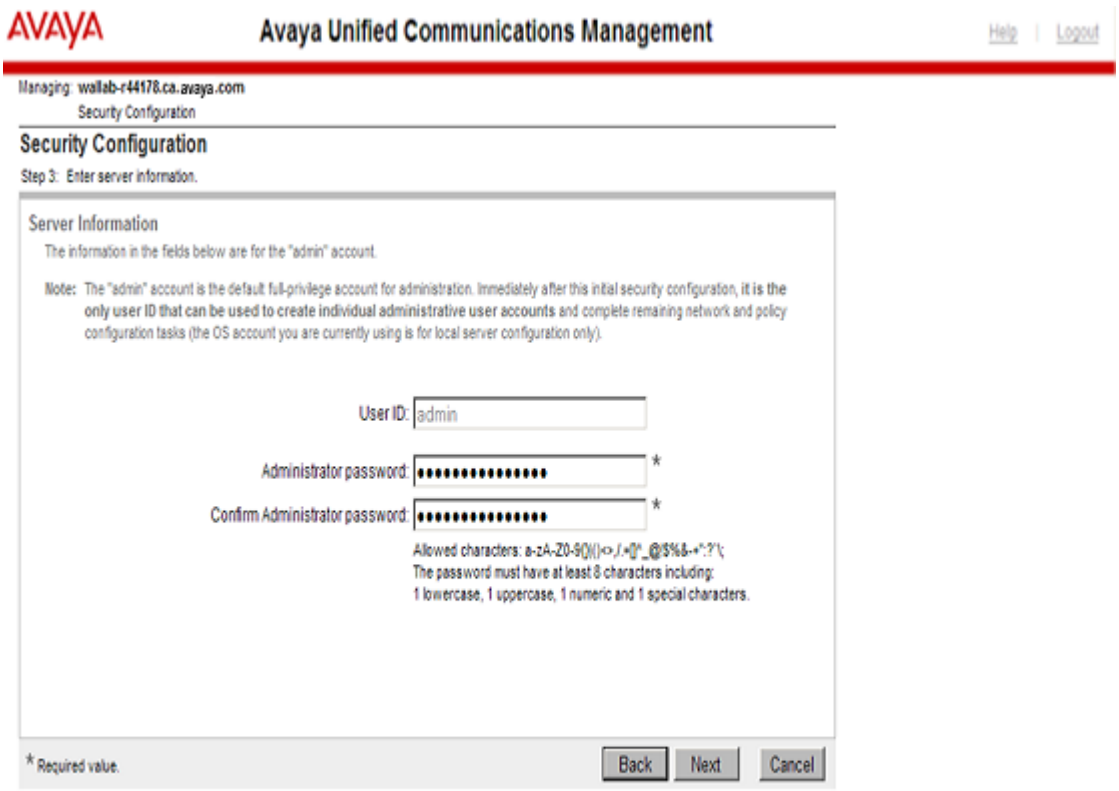
2. Click **Next**.

   The **Step 2: Select server type** page appears.



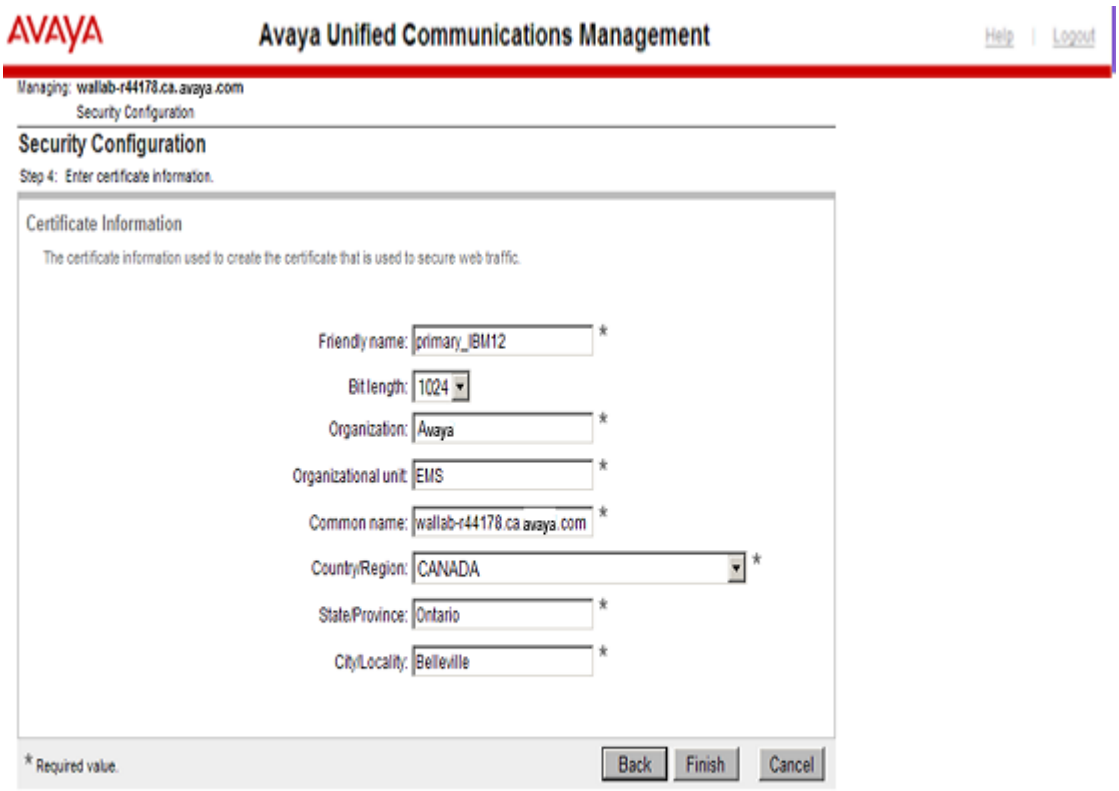
3. Select the **Primary security server** radio button and click **Next**.

   The **Step 3: Enter server information** page appears.



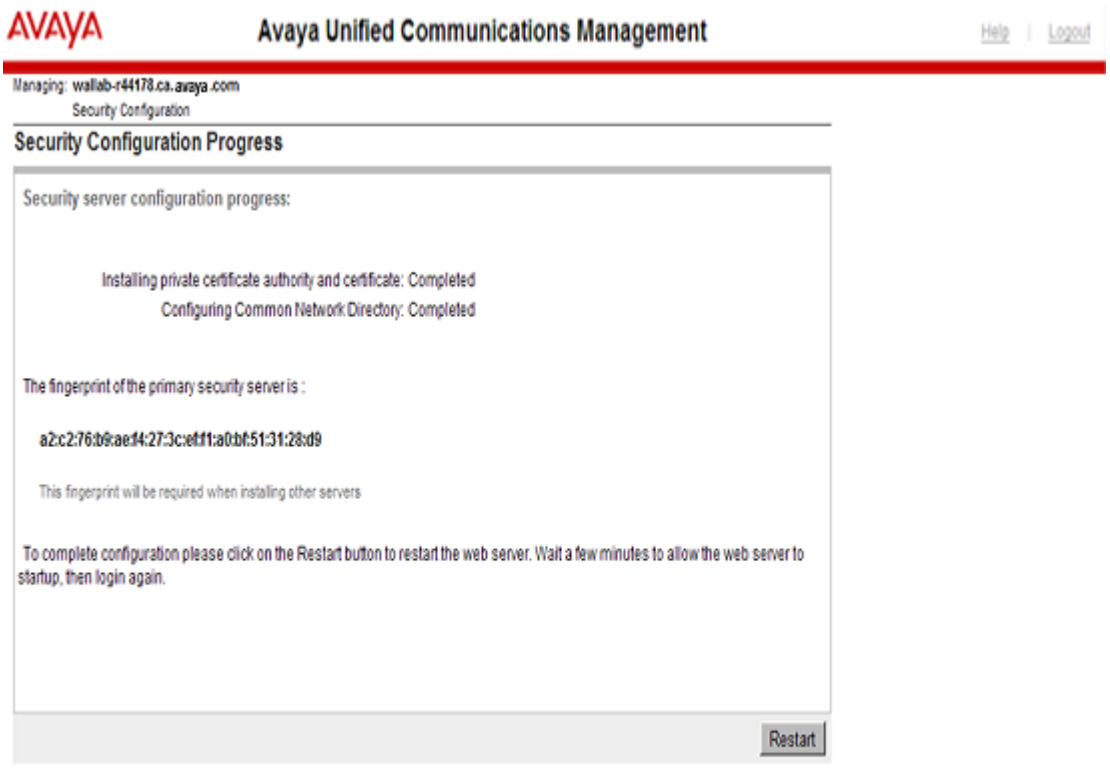
4. Enter the following information into the appropriate fields:
   - UserID
   - Administrator password
   - Confirm Administrator password
5. Click **Next**.

   The **Step 4: Enter certificate information** page appears.

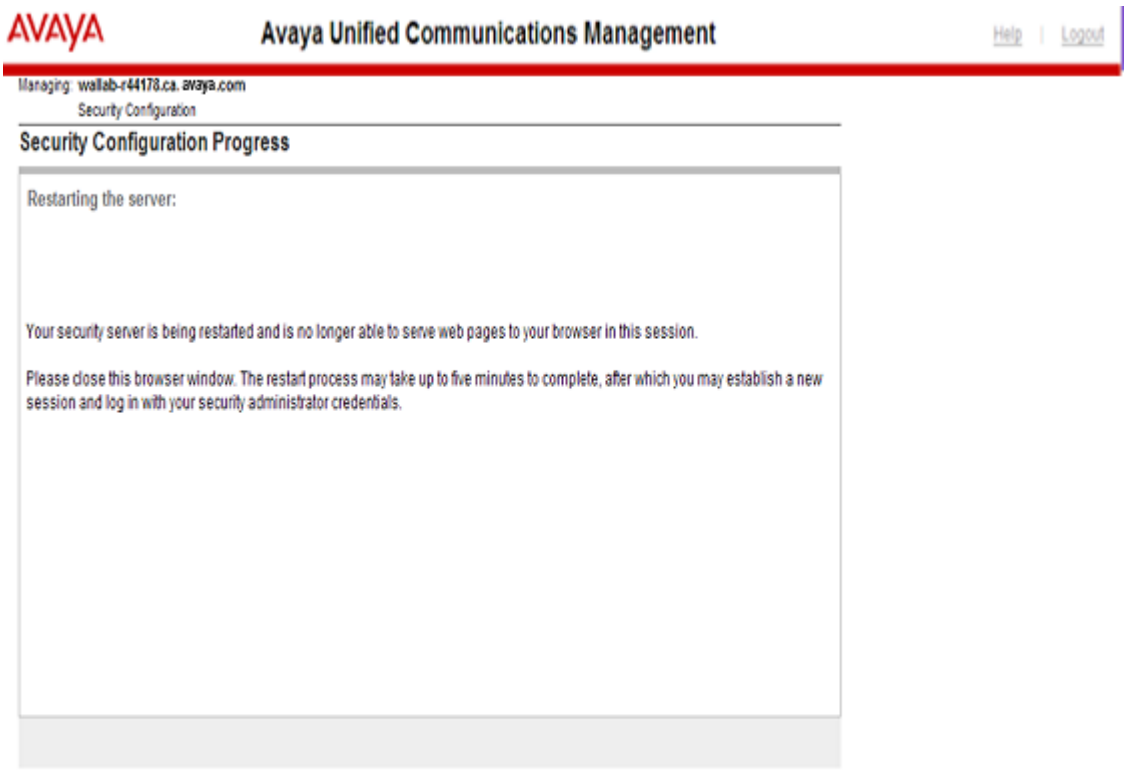


6. Enter the following information into the appropriate fields:
   - Friendly name
   - Bit length
   - Organization
   - Organizational unit
   - Common name
   - Country/Region
   - State/Province
   - City/Locality
7. Click **Finish**.

   The **Security Configuration Progress** page appears.



8. To complete the configuration process, you must restart the web server. Click **Restart**.
   The **Security Configuration Progress** page confirms that the server is restarting.

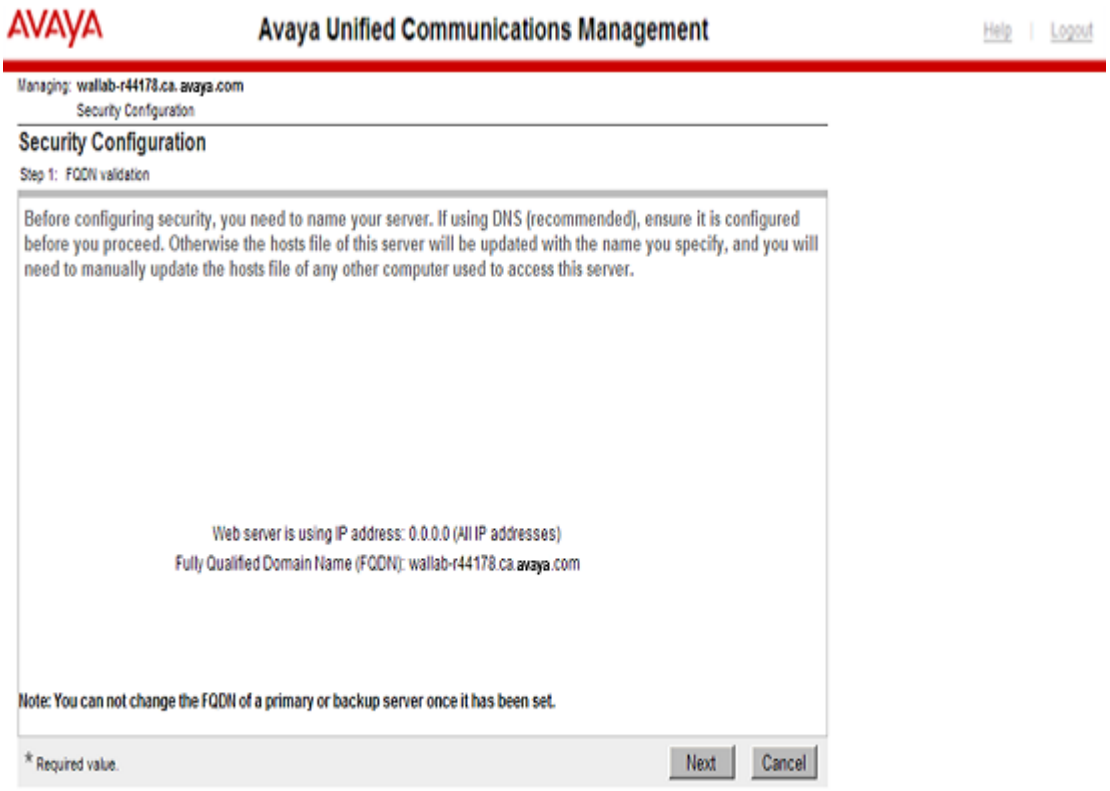


The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

Joining a Backup security server to the UCM security domain using Base Manager

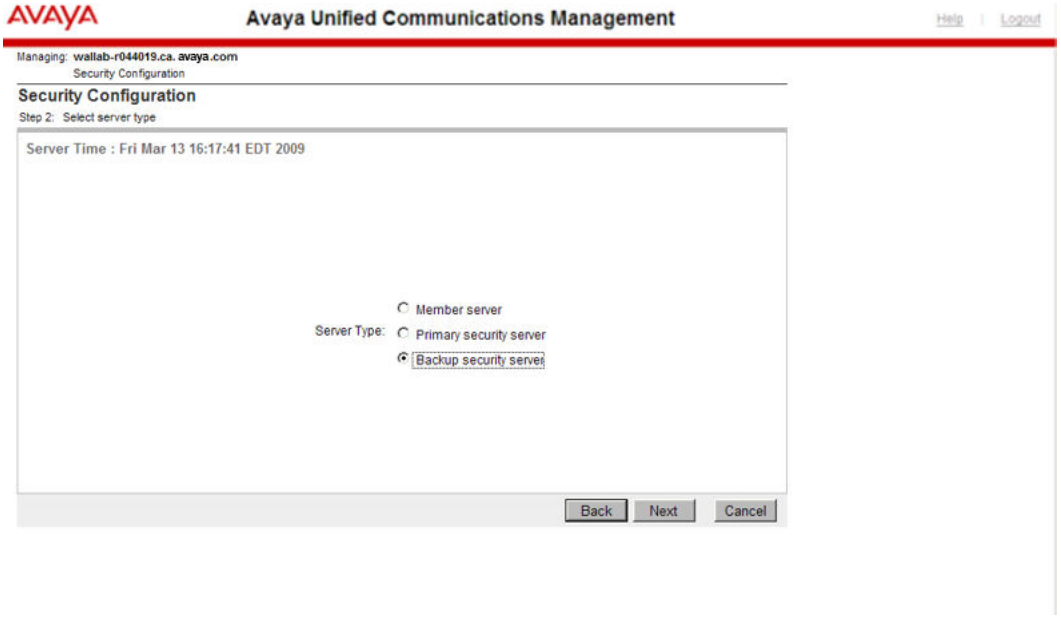
1. From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**.

   The **Step 1: FQDN validation** page appears.



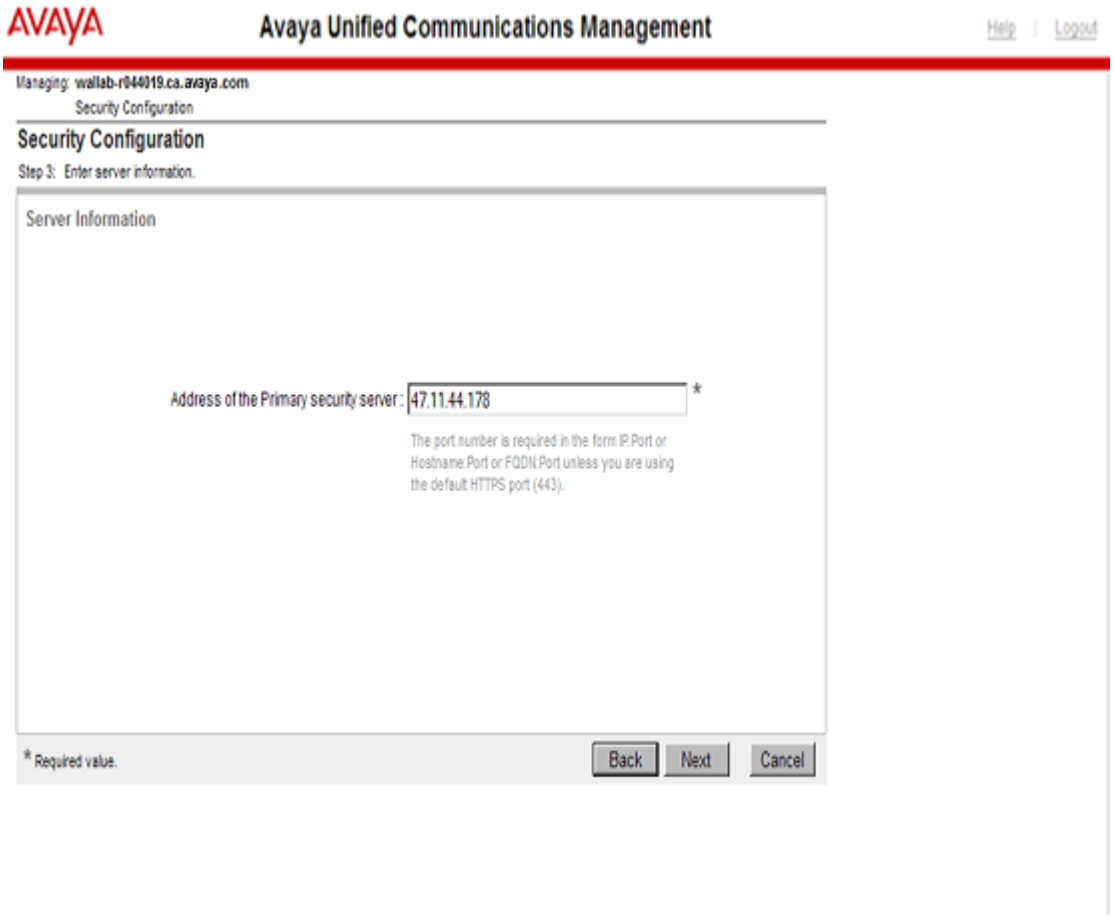
2. Click **Next**.

   The **Step 2: Select server type** page appears.



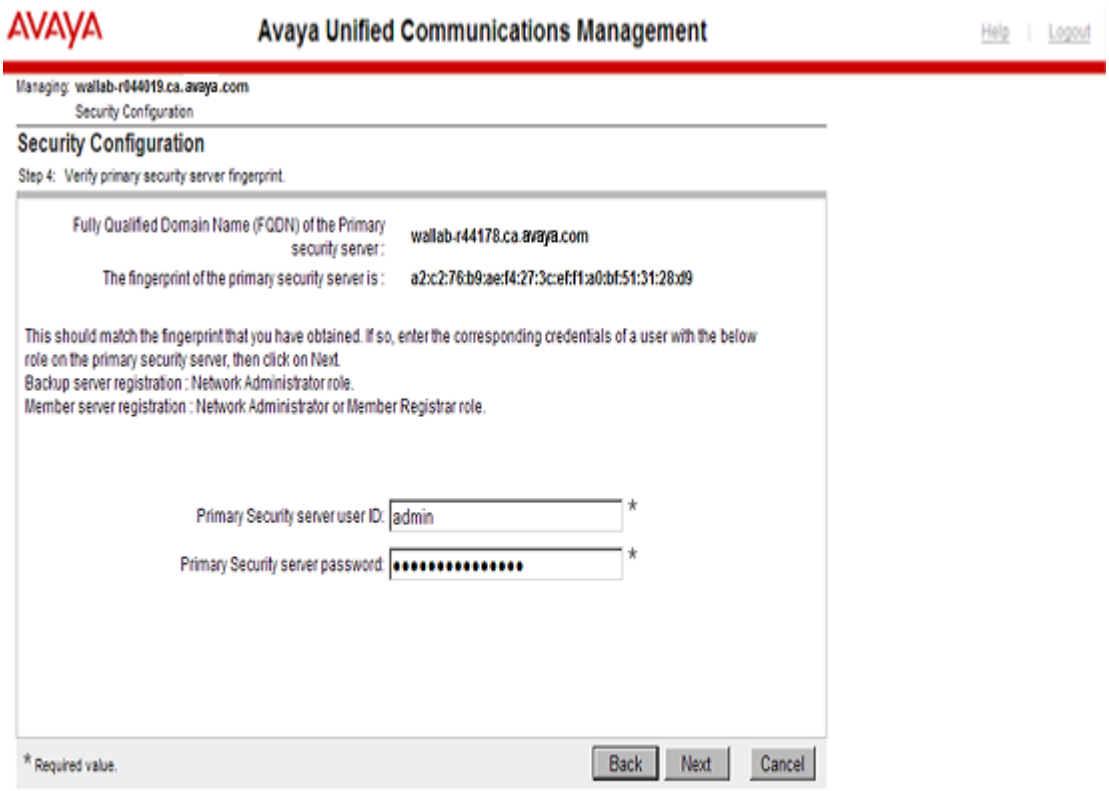
3. Select the **Backup security server** radio button and click **Next**.

   The **Step 3: Enter server information** page appears.



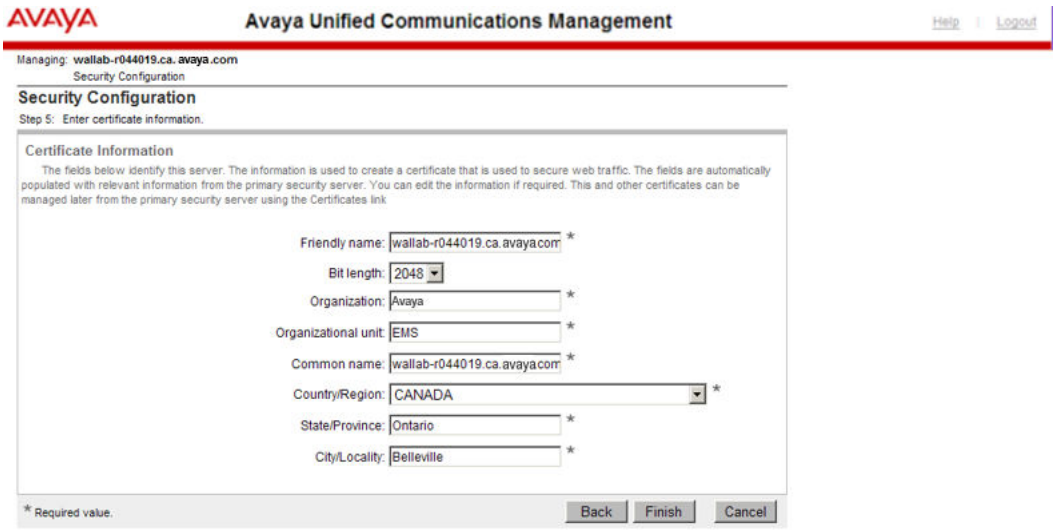
4. Enter the IP address of the Primary security server and click **Next**.

   The **Step 4: Verify primary security server fingerprint** page appears.



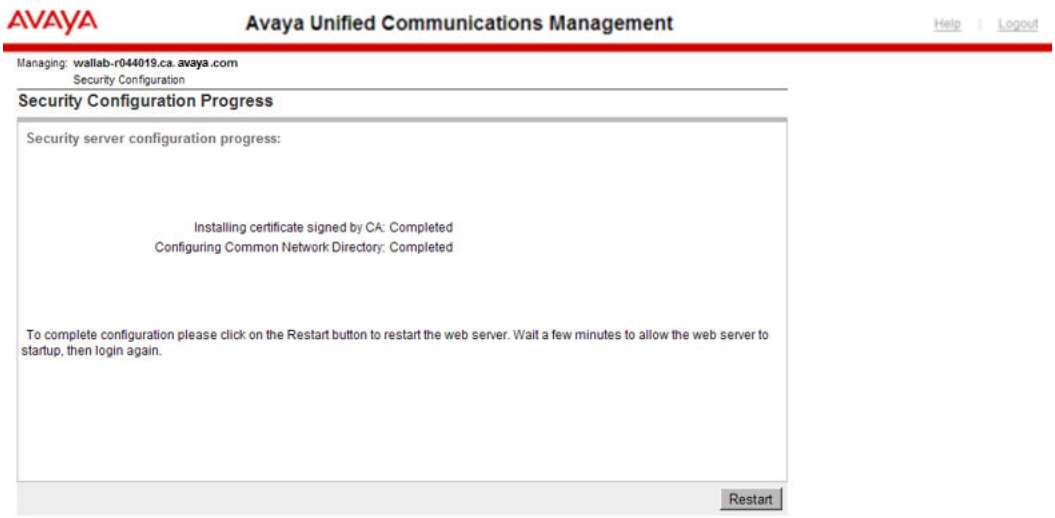
5. Verify that the FQDN and fingerprint information for the primary security server is valid and enter the following into the appropriate fields:
   - Primary Security server user ID
   - Primary Security server password
6. Click **Next**.

   The **Step 5: Enter certificate information** page appears.

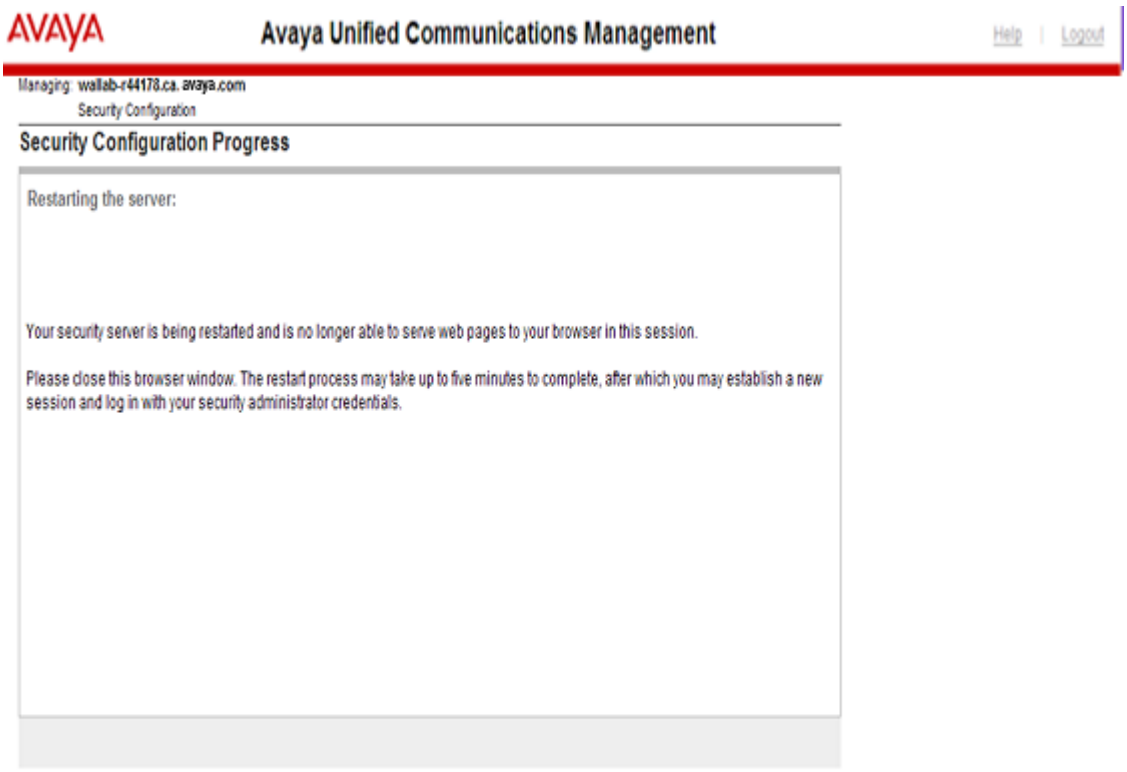


7. Enter the following information into the appropriate fields:
   - Friendly name
   - Bit length
   - Organization
   - Organizational unit
   - Common name
   - Country/Region
   - State/Province
   - City/Locality
8. Click **Finish**.

   The Security Configuration Progress page appears.



9. To complete the configuration process, you must restart the web server. Click **Restart**.
   The **Security Configuration Progress** page confirms that the server is restarting.

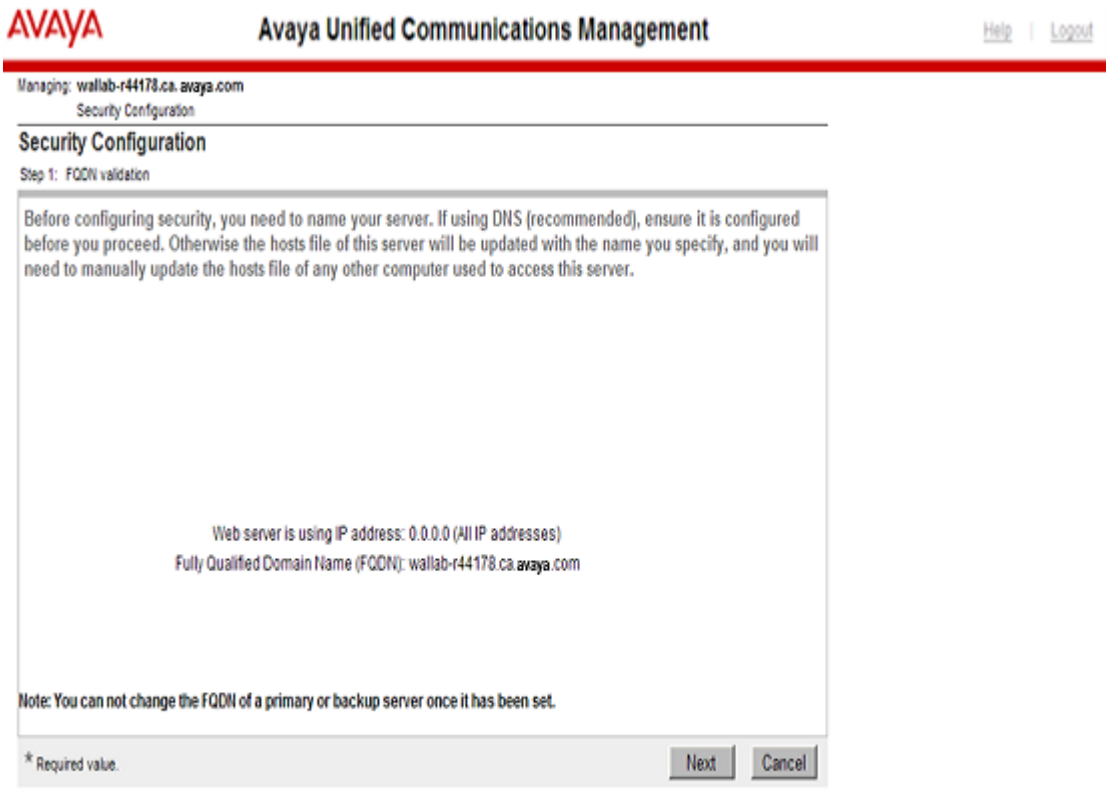


The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

Joining a member server to the UCM security domain using Base Manager

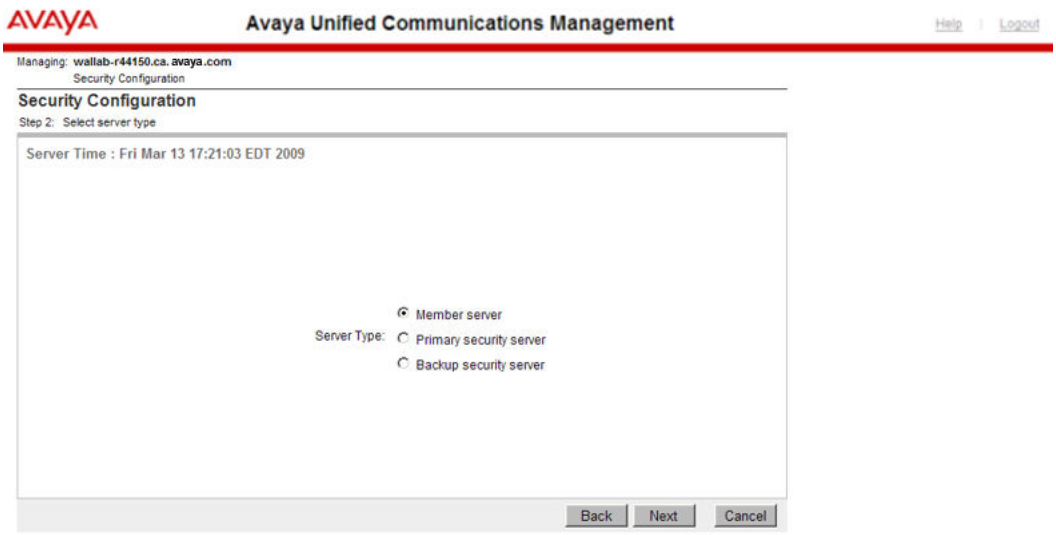
1. From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**.

   The **Step 1: FQDN validation** page appears.



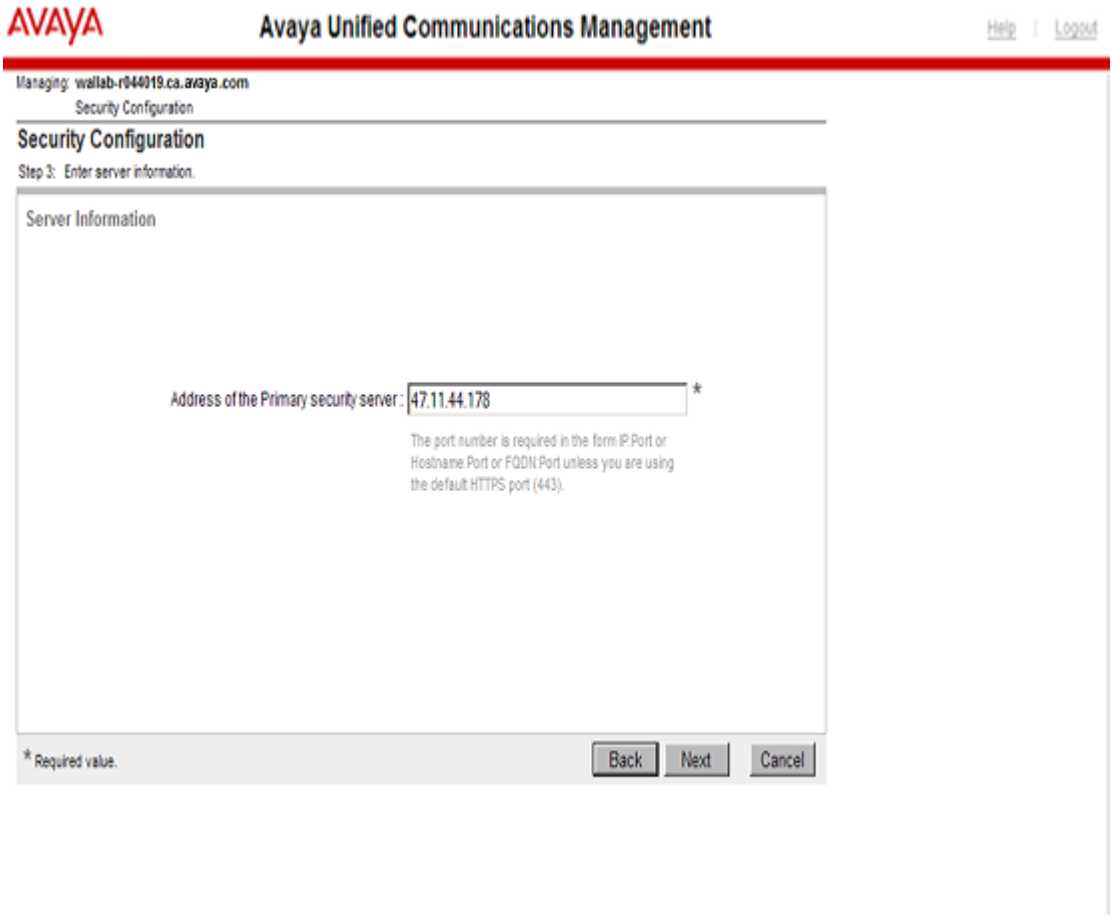
2. Click **Next**.

   The Step 2: Select server type page appears.



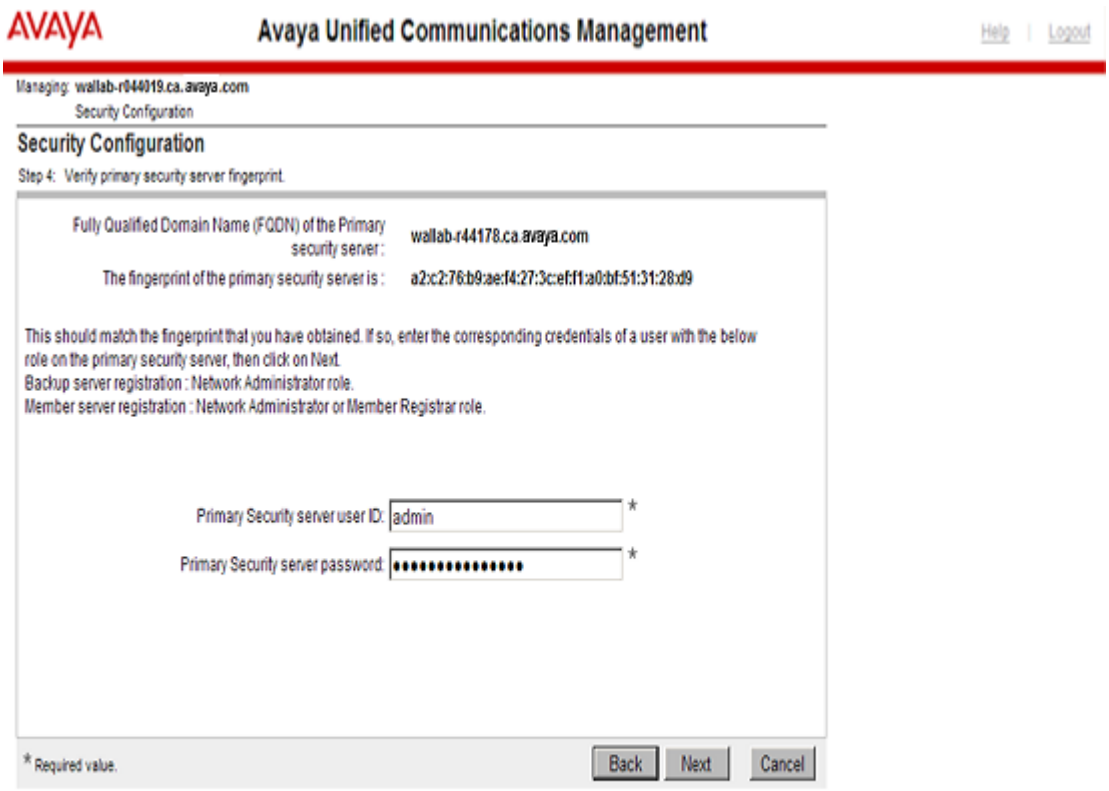
3. Select the **Member server** radio button and click **Next**.

   The **Step 3: Enter server information** page appears.



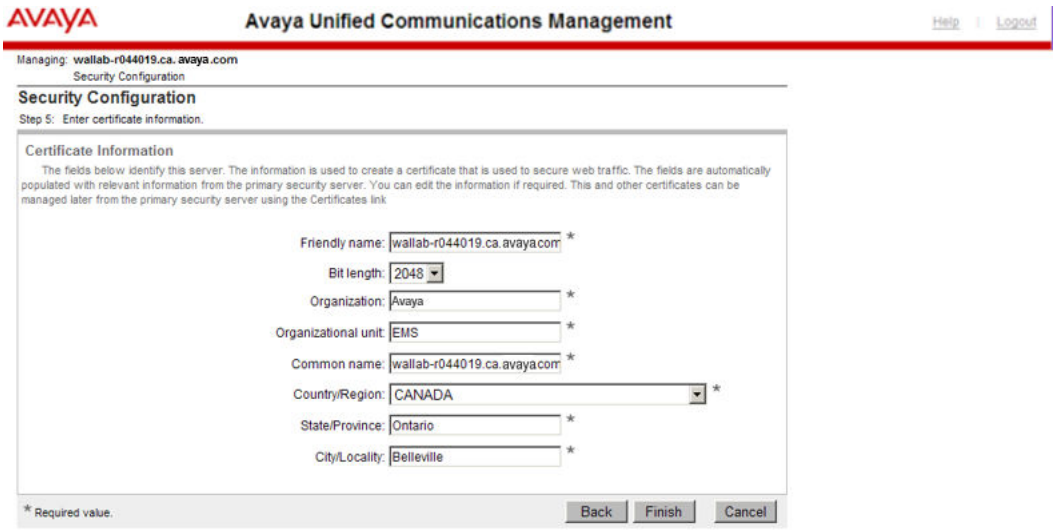
4. Enter the IP address of the Primary security server and click **Next**.

   The **Step 4: Verify primary security server fingerprint** page appears.



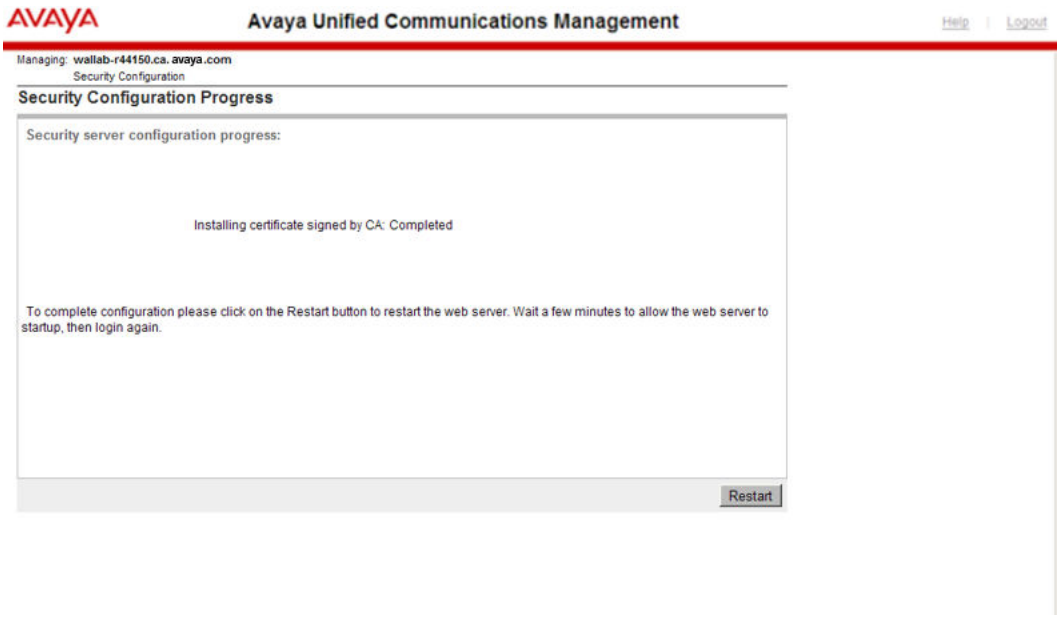
5. Verify that the FQDN and fingerprint information for the primary security server is valid and enter the following into the appropriate fields:
   - Primary Security server user ID
   - Primary Security server password
6. Click **Next**.

   The **Step 5: Enter certificate information** page appears.

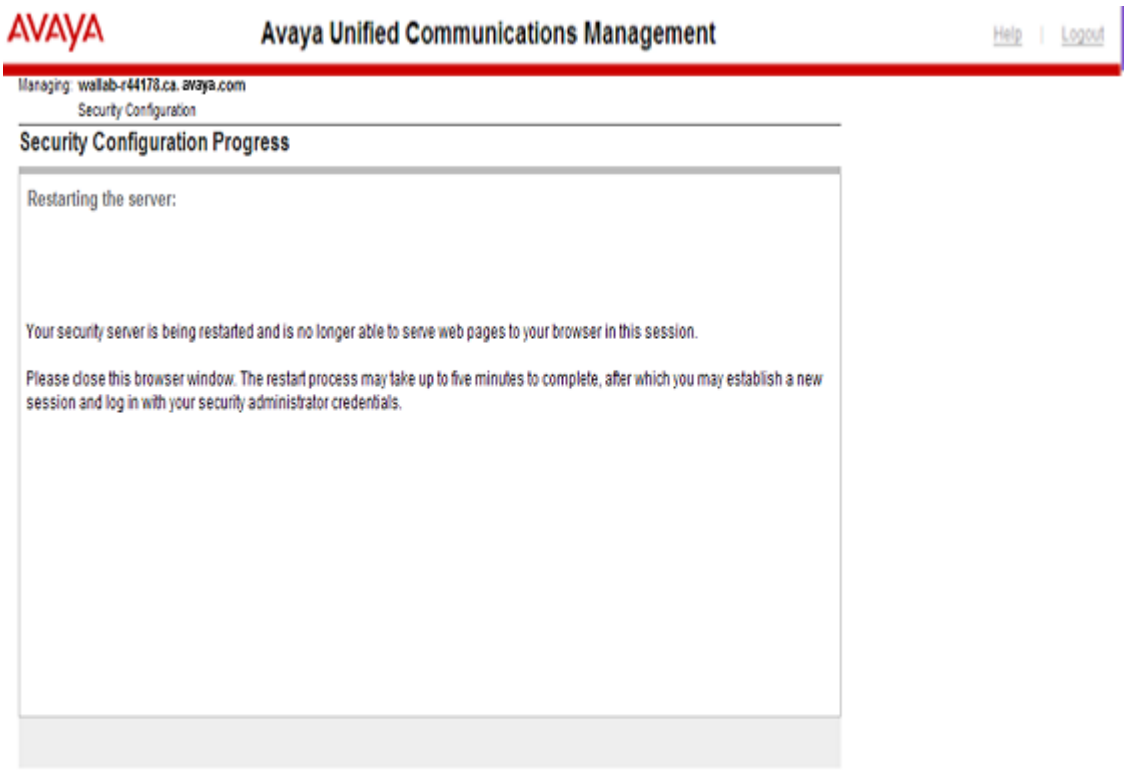


7. Enter the following information into the appropriate fields:
   - Friendly name
   - Bit length
   - Organization
   - Organizational unit
   - Common name
   - Country/Region
   - State/Province
   - City/Locality
8. Click **Finish**.

   The Security Configuration Progress page appears.



9. To complete the configuration process, you must restart the web server. Click **Restart**.
   The **Security Configuration Progress** page confirms that the server is restarting.



The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

Redundant systems

Note:

High Availability (HA) Call Servers must be in redundant mode to properly register to the security domain. If the Call Server is split for any reason, it must re-register to the security domain once a successful join command is issued.

Redundant systems can join the Unified Communications Management security domain using the following modes:

- Redundant mode—the joining and leaving of the Unified Communications Management security domain operation is mirrored between the active and inactive cores, where the LD 117 commands must be issued from the active server.
  - LD 117 command: **`[REGISTER / UNREGISTER] UCMSECURITY [DEVICE / SYSTEM]`**

- Split mode—the joining and leaving of the Unified Communications Management security domain operation is performed independently by the active and inactive cores.
  - LD 117 commands available on active core: **[REGISTER / UNREGISTER] UCMSECURITY [SYSTEM / DEVICE]**

    The joining and leaving of the Unified Communications Management security domain operation is mirrored between the active and inactive cores. The register/unregister commands apply only to the active core and its associated devices and the inactive core remains unregistered.
  - LD 117 commands available on inactive core: **[REGISTER / UNREGISTER] UCMSECURITY DEVICE**

    Do not issue registration commands from the inactive core except as part of a diagnostic process.
- Single mode—if required, you can use the unregister commands while in single mode. You should not issue registration commands from an HA system when in single mode. In single mode, both cores identify themselves as the active CPU when connected to the LAN. You should restore HA redundancy prior to attempting registration with the security domain.

Move an element from one UCM security domain to another

This section contains information about moving an element from one UCM security domain to another UCM security domain. This section contains the following procedures:

- Moving a Linux member element to another UCM security domain on page 251
- Moving a single VxWorks element to another UCM security domain on page 252
- Moving all VxWorks elements on a Call Server to another UCM security domain on page 253

Moving a Linux member element to another UCM security domain

Perform the steps in this procedure if you are moving a Linux member element from one UCM security domain to another UCM security domain.

1. Log on to the Linux member element using the local login credentials.
2. From the Linux element CLI, perform the appropriate security configuration
3. When prompted, enter the IP address of the new UCM primary security server.
4. Log on to the former UCM primary security server for the Linux element as a user with security administrator privileges.
5. From the navigation tree, click **Elements**.

   The Elements Web page appears.

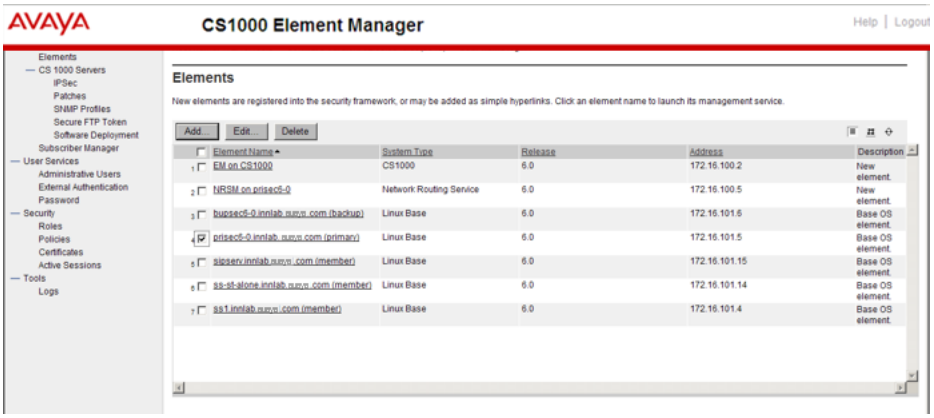


Figure 18: Elements Web page in UCM

6. From the list of elements, select the check box beside the Linux element that has been moved.
7. Click **Delete**.

Moving a single VxWorks element to another UCM security domain

Follow the steps in this procedure to move a single VxWorks element on a Call Server from one UCM security domain to another.

1. On the Call Server, decommission the VxWorks element that is being moved.
2. (Optional) From the element CLI, issue the LD 117 command **`unregister ucmsecurity system`** to remove the device from the UCM security domain.
3. From the element CLI, reconfigure the element using the local setup command.
4. Provision the element on the new Call Server, as required.
5. From the CLI of the device or the CLI of the Call Server, register the element to the UCM security domain by issuing the LD 117 command **`register ucmsecurity system`**.

   When prompted, confirm that the element is to be added to the UCM security domain.
6. Log on to the previous UCM primary security server as a user with security administrator privileges.
7. From the navigation tree, click **Elements**.

   The Elements Web page appears, as shown in Figure 18: Elements Web page in UCM on page 252.
8. From the list of elements, select the check box beside each element that has been moved.
9. Click **Delete**.

Moving all VxWorks elements on a Call Server to another UCM security domain

Follow the steps in this procedure to move all VxWorks elements on a Call Server from one UCM security domain to another.

1. (Optional) From the Call Server CLI, issue the LD 117 command **`unregister ucmsecurity system`** to remove all devices registered to the Call Server from the UCM security domain.
2. From the Call Server CLI, issue the LD 117 command **`register ucmsecurity system`** .
3. Specify the IP address of the new UCM primary security server and the credentials for registering with the UCM security domain.
4. Log on to the previous UCM primary security server as a user with security administrator privileges.
5. From the navigation tree, click **Elements**.

   The Elements Web page appears, as shown in Figure 18: Elements Web page in UCM on page 252.
6. From the list of elements, select the check box beside each element that has been moved.
7. Click **Delete**.

Authentication methods

The following methods are used for authenticating users and devices on the Communication Server 1000 network.

Central authentication

Unified Communications Management operates at the security domain level and centrally manages and authenticates users and their permissions. When a Communication Server 1000 element joins the UCM security domain, system management and support users log in with accounts defined in UCM, which then authenticates the user based on the password provided and authorizes the functionality that can be accessed based on the permissions that the user has been assigned.

UCM implements role-based access control, which enables a set of permissions to be bundled together into a role. A user obtains permissions to perform various functions by being assigned one or more roles. For information about roles in UCM, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Standalone systems that have not joined the UCM security domain can still use their local authentication and authorization methods. When a Communication Server 1000 Call Server has not joined the security domain, system management and support users log in to the ADMIN, ADMIN2, PDT1, PDT2 and various LAPW accounts. The Call Server locally authenticates the account based

on the password provided and authorizes the functionality that can be accessed based on the account permissions. Similarly, when a Communication Server 1000 Signaling Server has not joined the security domain, users log in to the OAM and PDT accounts and the Signaling Server provides local authentication and authorization.

Switch to local authentication

In the event that an element belongs to the UCM security domain and access to the Primary or Secondary UCM Security Server is interrupted, or a device is removed from the security domain, users with network administrator permissions can still access local elements using local authentication and authorization methods.

To reset authentication to local, follow the steps in Switching to local authentication on page 254.

Switching to local authentication

1. At the device CLI, enter CTRL-P, CTRL-D, CTRL-T to start PDT.

   Do not enter your UserID at the prompt.

2. At the prompt, enter the authentication reset command:

   `resetCAUTH`

   The authentication reset initiates and a message appears stating that you must load the installation media into the removable media drive within 60 seconds.

3. Load the installation media into the removable media drive.

   Once the installation media is confirmed, the authentication type is set to LOCAL.

4. Remove the installation media and, if prompted, insert any backup media.

To rejoin a device to the UCM security domain, you must issue the appropriate command, as described in Add or remove elements from the UCM security domain on page 227.

Secure UserID and password authentication with a system security token

A system security token is a randomly generated block of data that generates an algorithm for the creation of a unique password. This password is associated with a specific UserID and is unique to the installation. The data provided by the Unified Communications Management primary security server is used by the system to calculate unique passwords for each of the accounts used by the NFC API (Network File Copy Application Programming Interface), a module contained within the application source code that supplies hardcoded UserIDs and passwords when file transfer requests are made.

The Unified Communications Management primary security server distributes a system-wide security token to elements as they are registered. A security administrator can modify the token from the Unified Communications Management primary security server or schedule the token for modification at periodic intervals. The modified token is then transferred to all registered elements.

The token is transferred to the member servers with best-effort, with attempts made every five minutes until the operation succeeds. The security tokens are transferred using sFTP. If the token

on a network element does not match the token distributed by the Unified Communications Management primary security server, sFTP fails.

From the Secure FTP Token Management page in Unified Communications Management, you can refresh the status of the current token or regenerate a new token for distribution throughout the network.

Note:

The token is backed up during Linux base backup procedures and restored during Linux base upgrades.

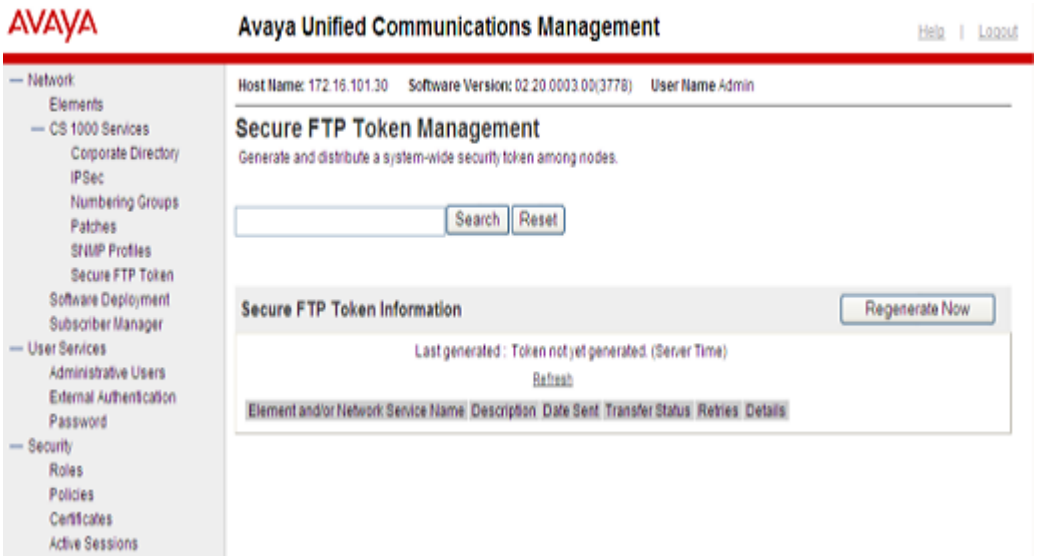
Regenerate the Secure FTP Token

You can use the Secure FTP Token Management page on the UCM security server to validate a successful registration by regenerating and distributing the secure token to all elements in the security domain. Use this procedure to regenerate the Secure FTP token.

Regenerating the Secure FTP Token

1. Log on to the UCM primary security server.
2. Navigate to **Network > CS 1000 Servers > Secure FTP Token**.

   The Secure FTP Token Management page appears.



3. Click **Regenerate Now**.

Refresh system keys

Several components of the Communication Server 1000 security solution make use of a public key certificate to ensure privacy. These certificates use a digital signature to bind together a public key

with an identity, enabling trusted communication without the need for regular exchange of secret keys between endpoints.

To enhance the security of your system, change your system keys periodically. Avaya 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 the following table.

Table 56: System keys that must be manually refreshed

Key	For more information, see:
SSH	Manage SSH keys using overlays on page 270 ORSSH key management using Element Manager on page 272
TLS	SIP TLS can use the same key as Element Manager. See *Avaya Element Manager System Reference — Administration, NN43001-632*
sFTP token	Secure UserID and password authentication with a system security token on page 254
Web SSL (HTTPS)	*Avaya Element Manager System Reference — Administration, NN43001-632*
N-Way redundancy	*Avaya Network Routing Service Fundamentals, NN43001-130*

When you refresh the SSH keys, SSH is unavailable until the new keys are generated. On most systems, this occurs almost instantaneously.

Control access to system Application Processors

Restrict access to Application Processors by requiring a user to enter a valid user name and password on the Application Processor console. The user can then access and run applications, or configure operating characteristics of the Application Processor.

System access privileges are based on user IDs that are password-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 on page 50.

Configure Secure File Transfer Protocol

Use the procedures in this section to configure Secure Shell (SSH) Secure File Transfer Protocol (sFTP).

Warning:

sFTP is enabled by default. Do not disable sFTP unless it is required for troubleshooting purposes. sFTP must remain enabled to ensure the successful operation of Communication Server 1000 systems.

sFTP configuration using overlays

Use the following LD 117 commands to configure sFTP on the Call Server.

Table 57: LD117 commands for enabling and disabling secure transport

Command	Preconditions	Description
ENL TRANSFERS INSECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands	• Enables insecure FTP for internal negotiation of elements on the system. • The Call Server sends a message by pbxLink to all

Table continues…

Command	Preconditions	Description
		connected devices and IPMG devices. • The device generates SEC0089, indicating insecure transfer is enabled.
ENL TRANSFERS SECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands	• Enables secure FTP for internal negotiation of elements on the system. • The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0087, indicating the host [host/subnet] is removed from the list of allowed hosts for SSH connection.
DIS TRANSFERS INSECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands • Secure transport has not been disabled. Insecure and secure transports cannot be disabled simultaneously.	• Disables insecure FTP for internal negotiation of elements on the system. • The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0090, indicating that insecure transfer is disabled.
DIS TRANSFERS SECURE	• PWD2 privilege • 5 minutes or longer after previously issued ENL/DIS commands • Secure transport has not been disabled. Insecure and secure transports cannot be disabled simultaneously.	• Disables secure FTP for internal negotiation of elements on the system. • The Call Server sends a message by pbxLink to all connected devices and IPMG devices. • The device generates SEC0088, indicating secure transfer is disabled.
STAT TRANSFERS INSECURE	None	Displays the insecure transport status
STAT TRANSFERS SECURE	None	Displays the secure transport status

System elements, such as Signaling Server, Gateway Controller, and ITG-SA, have access to their local shell commands to enable or disable the secure or insecure transfers, as well as the stat

commands. The enable, disable, and stat commands are provided on the OAM and PDT2 shells and only users with PWD2 rights can execute them.

Table 58: OAM and PDT2 shell commands for enabling and disabling secure transport

Command	Preconditions	Description
disInsecureTransfers	PWD2 privilege	Disables insecure FTP for internal negotiation of elements on the system.
enlInsecureTransfers	PWD2 privilege	Enables insecure FTP for internal negotiation of elements on the system.
disSecureTransfers	PWD2 privilege	Disables secure FTP for internal negotiation of elements on the system.
enlSecureTransfers	PWD2 privilege	Enables secure FTP for internal negotiation of elements on the system.
statInsecureTransfers	PWD2 privilege	Displays whether insecure transfer access is enabled or disabled.
statSecureTransfers	PWD2 privilege	Displays whether secure transfer access is enabled or disabled.

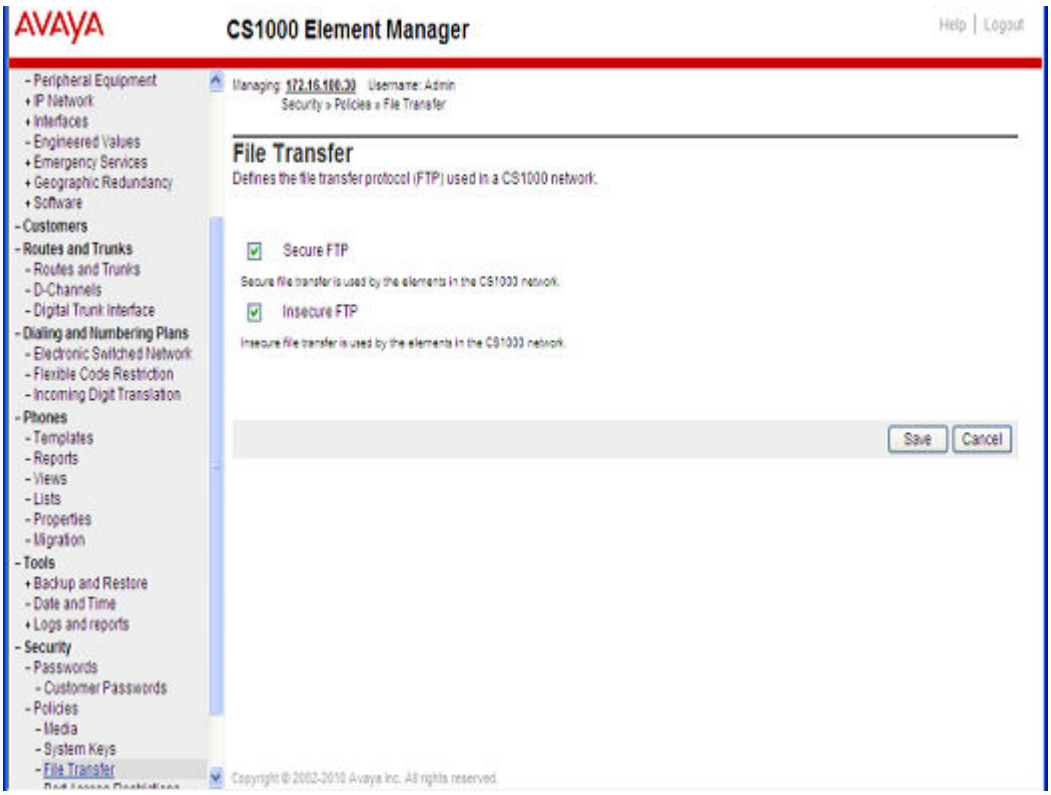
sFTP configuration using Element Manger

Use this procedure to configure sFTP using Element Manager.

Configuring file transfer options using Element Manager

1. Log on to Element Manager as a user with security administrator privileges.
2. Navigate to **Security > Policies > File Transfer**.

   The File Transfer page displays. By default, the **Secure FTP** and **Insecure FTP** boxes are both selected.



3. Select or deselect the desired file transfer option. At least one option must be selected or an error message appears.
4. Click **Save**.

   You can also click **Cancel** to discard the changes.

   Note:

   If you make changes to the file transfer options, you must wait at least 5 minutes before attempting to modify the settings again. Otherwise, an error message appears.

Configure port access restrictions

This section provides information about configuring port access restrictions using overlays or Element Manager.

Port Access Restrictions configuration page

You can use Element Manager to configure port access restrictions. To view the port access restrictions details, log on as a user with Security Administrator permissions and navigate to **Security > Policies > Port Access Restrictions**.

The Port Access Restrictions page is shown in Figure 19: Port Access Restrictions page in Element Manager on page 261 with the Default rules selected.

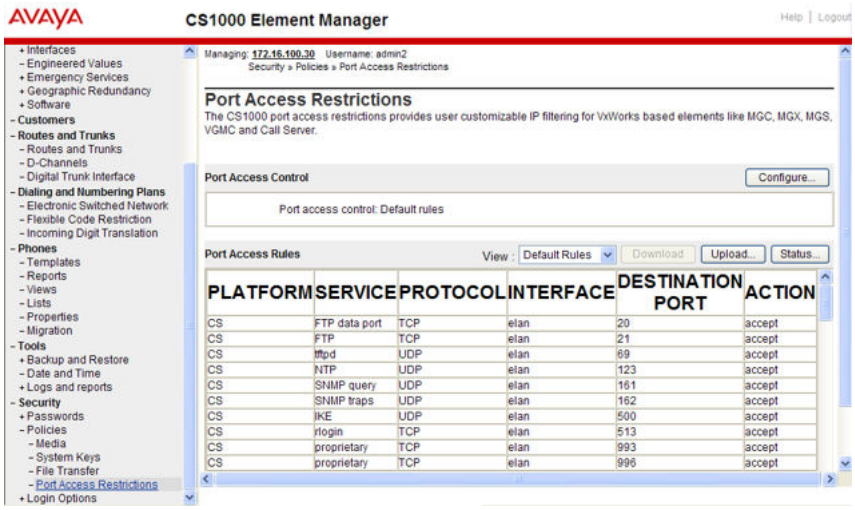


Figure 19: Port Access Restrictions page in Element Manager

The Port Access Restrictions page has two main sections:

- Port Access Control—this section indicates whether the current access restriction rules are configured as Default, Custom, or None.
- Port Access Rules—this section displays the current access restriction rules.

From this page you can do the following tasks:

- Configure port access rules
- View the current rules status
- Upload a custom rules file
- Download a custom rules file (this option is only available if a custom rules XML file exists)

For procedures related to port access restrictions and Element Manager, see Configure port access restrictions using Element Manager on page 263.

Backing up and restoring port access restrictions

To save changes to the port access restrictions configuration settings, you must perform a data dump on the Call Server. The state of the port blocker (off, default, custom) is also saved when a data dump is performed on the Call Server. The default rules file does not get data dumped because it is installed during upgrade.

You can only backup or restore the custom rules file.

System wide administration commands in LD 117

The following system wide administration commands are available in LD 117. All port access commands require that you have SEC_ADMIN user role privileges.

Table 59: Access restrictions system wide administration commands in LD 117

Command	Description
PORT ACCESS CUSTOM	This command loads the custom port access rules that were uploaded using Element Manager or by FTP. If a custom file exists, the following prompt displays on the console: `Enabling a CUSTOM file could possibly have detrimental effects to the system. Are you sure you want to continue this process? (Yes/[No])` Respond yes to accept the change or no to deny it. If you respond yes, the system verifies the custom file is valid before attempting to load the rules. If the file fails to load, the state will be set back to its previous. If the custom file loads successfully, the Call Server sends a custom state message to all Gateway Controllers, MC32S, and any inactive Call Server core endpoints to download the files (if necessary) and change their configuration to custom. A datadump is required to save the state.
PORT ACCESS DEFAULT	This command loads the default port access rules stored in a file during installation. If other port access rules are active, those rules are deactivated first. If the default rule file activates successfully, the state on the Call Server changes to default. The Call Server sends a default state message to all Gateway Controllers, MC32S, and any inactive Call Server core endpoints to download the file (if necessary) and change their configuration to default. A datadump is required to save the state.
PORT ACCESS OFF	This command disables access restrictions on the Call Server and sends an off state message to all Gateway Controllers, MC32S, and any inactive Call Server core endpoints to change their configuration to off. A datadump is required to save the state.
PORT ACCESS STATUS [ALL / DEBUG]	This command displays the global state of the Access Restrictions. If the DEBUG option is selected, it will also show default and custom signatures with the global status. If the ALL option is selected, it polls the endpoints to detect the local status and lists all cards that do not have matching file signatures or cannot be contacted.

Table continues…

Command	Description
	If all cards match, a message states that all endpoints match will be displayed.
PORT ACCESS VALIDATE	This command validates a custom file, prints out any errors detected, and provides possible fixes.
PORT ACCESS SHOW DEFAULT	This command displays the rules of the default file in tabular format.
PORT ACCESS SHOW CUSTOM	This command displays the rules of the custom file in tabular format.

Configure port access restrictions using Element Manager

This section provides information about configuring port access restrictions using the Element Manager interface.

Configuring port access restrictions using Element Manager

1. Log on to Element Manager as a user with Security Administrator privileges.
2. Navigate to **Security > Policies > Port Access Restrictions**.
3. Click **Configure**.

   The Port Access Control Details page appears, as shown in Figure 20: Element Manager Port Access Control Details page on page 263.

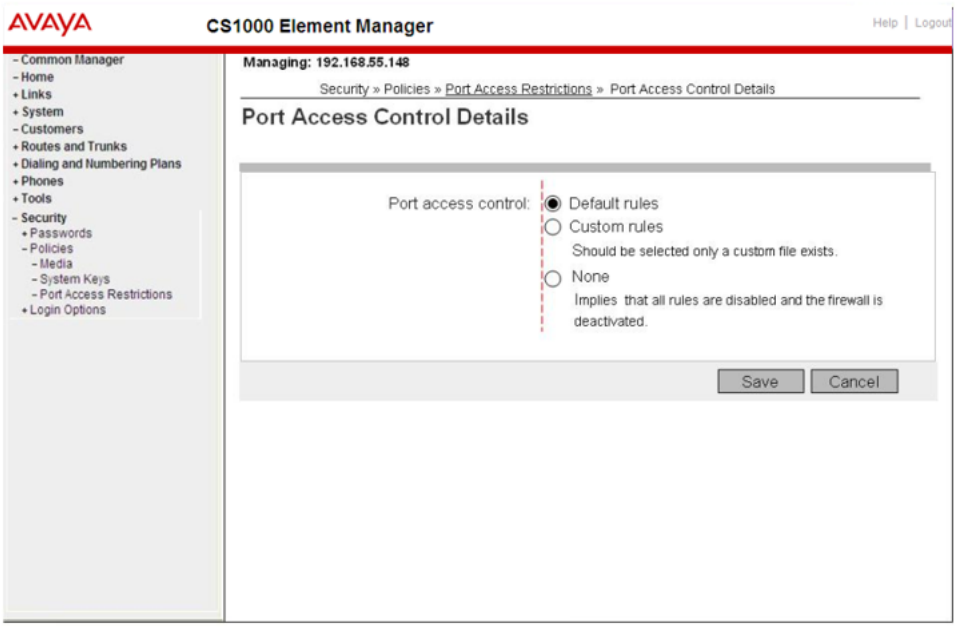


Figure 20: Element Manager Port Access Control Details page

4. Select an option from the Port access control rules list. The following options are available:
   - Default rules—the system default configurations
   - Custom rules—select this option only if a Custom settings file exists
   - None—selecting this rule implies that all rules are disabled (except for the mandatory system rules) and that the firewall is deactivated

   If you select the Custom rules option, a confirmation message displays. Click **OK** to accept or **Cancel** to return to the list and make another selection.
5. Click **Save**.

   You can also click **Cancel** to discard the changes.

Download the custom rules template file using Element Manager

Use this procedure to download the custom rules template file (template.xml).

Downloading the custom rules template file using Element Manager

1. Log on toElement Manager as a user with Security Administrator privileges.
2. Navigate to **Security > Policies > Port Access Restrictions**.

   The Port Access Restrictions page appears.
3. In the Port Access Rules section, verify that the View selection is blank (no selection).
4. Click **Download**.
5. Save the custom rules template file to the local machine. From the browser menu, select **File > Save as**.

Download the custom rules file using Element Manager

Use this procedure to download the custom rules file.

Downloading a custom rules file using Element Manager

1. Log on to Element Manager as a user with Security Administrator privileges.
2. Navigate to **Security > Policies > Port Access Restrictions**.

   The Port Access Restrictions page appears.
3. In the Port Access Rules section, verify that the View selection is Custom.
4. Click **Download**.

   A browser window opens displaying the contents of the custom XML file.
5. Save the custom file to the local machine. From the browser menu, select **File > Save as**.

Upload a custom rules file using Element Manager

Use this procedure to upload a customs rule file.

Uploading a custom rules file using Element Manager

1. Log on to Element Manager as a user with Security Administrator privileges.
2. Navigate to **Security > Policies > Port Access Restrictions**.

3. Click **Upload**.
4. The Upload Port Access Rules page appears, as shown in Figure 21: Element Manager Upload Port Access Rules page on page 265.

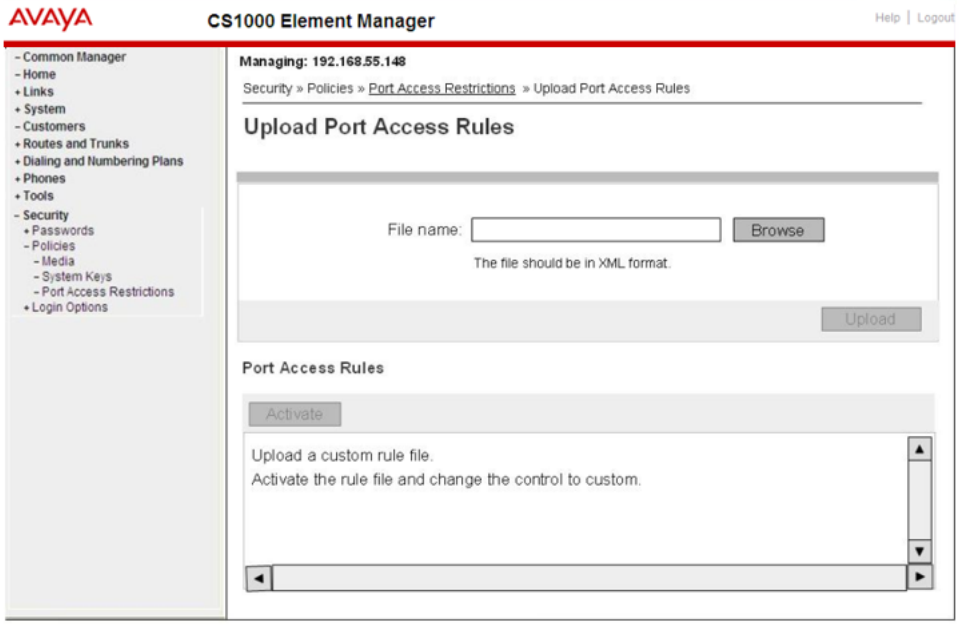


Figure 21: Element Manager Upload Port Access Rules page

5. Click **Browse** to select the custom rules file to upload.

   Note:

   The upload file must be in XML format and must have the following filename: customport.xml.

6. Click **OK** to upload the selected file.

   If the file is valid, the content of the custom rules file is displayed under the Port Access Rules section and the **Activate** button is enabled.

   If the upload fails, or if the file is invalid, an error message displays.

7. Click **Activate**.

   The uploaded custom file is activated and the Port Access Restrictions page displays.

View the port access restrictions status using Element Manager

Use this procedure to view the current port access restrictions status.

Viewing the port access restrictions status using Element Manager

1. Log on to Element Manager as a user with Security Administrator privileges.
2. Navigate to **Security > Policies > Port Access Restrictions**.
3. Click **Status**.

A wait message appears. The status operation can take a few minutes or longer, depending on the number of elements registered to the Call Server.

A new window opens and displays the current local and global port access restrictions status, as shown in Figure 22: Port access restrictions status window on page 266.

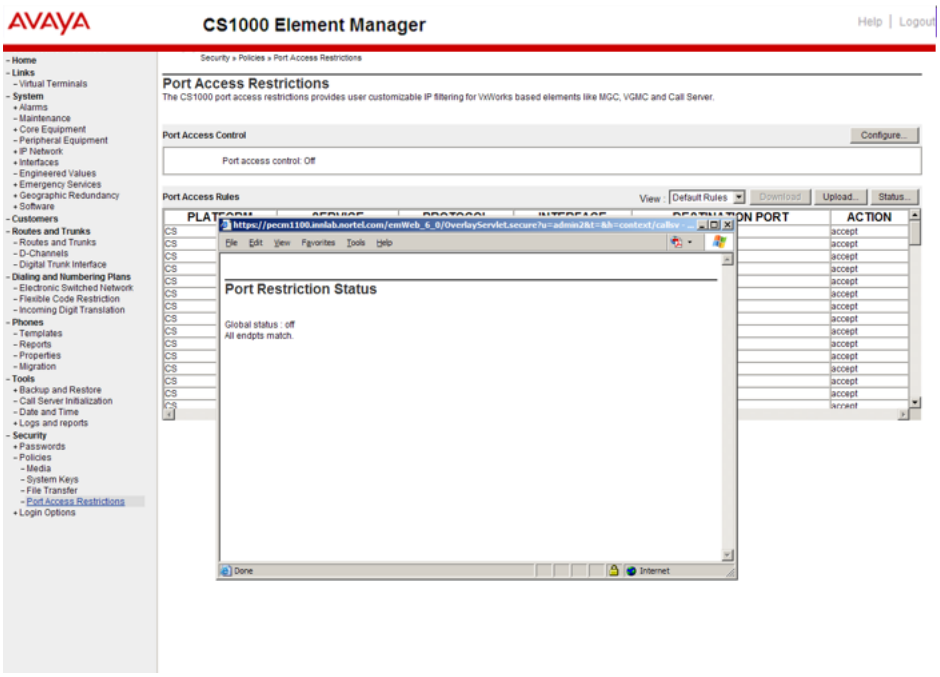


Figure 22: Port access restrictions status window

Configure remote access

This section provides information about configuring Remote Access using overlays or Element Manager.

Manage secure shell access from the Call Server using overlays

Use the following procedure to enable or disable Secure Shell (SSH) access, or to display the status of secure shell access.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Managing secure shell access by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 prompt, type one of the following commands:

   `ENL SHELLS SECURE` to enable secure shells

OR

`DIS SHELLS SECURE` to disable SSH.

OR

`STAT SHELLS SECURE` to display the status of SSH access.

For more information about the commands used in this procedure, see Table 60: Job aid: shell management commands in LD 117 on page 267.

Table 60: 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 60: Job aid: shell management commands in LD 117 on page 267.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Managing insecure shell access by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 prompt, type one of the following commands:

   `ENL SHELLS INSECURE` to enable insecure shells.

   OR

   `DIS SHELLS INSECURE` to disable insecure shells.

   OR

   `STAT SHELLS INSECURE` to display the status of insecure shell access.

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 61: Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices on page 268.

Managing insecure shell access by using CLI

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 61: Job aid: insecure shell management commands on Signaling Server and Voice Gateway Media Card devices on page 268.

Table 61: 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.

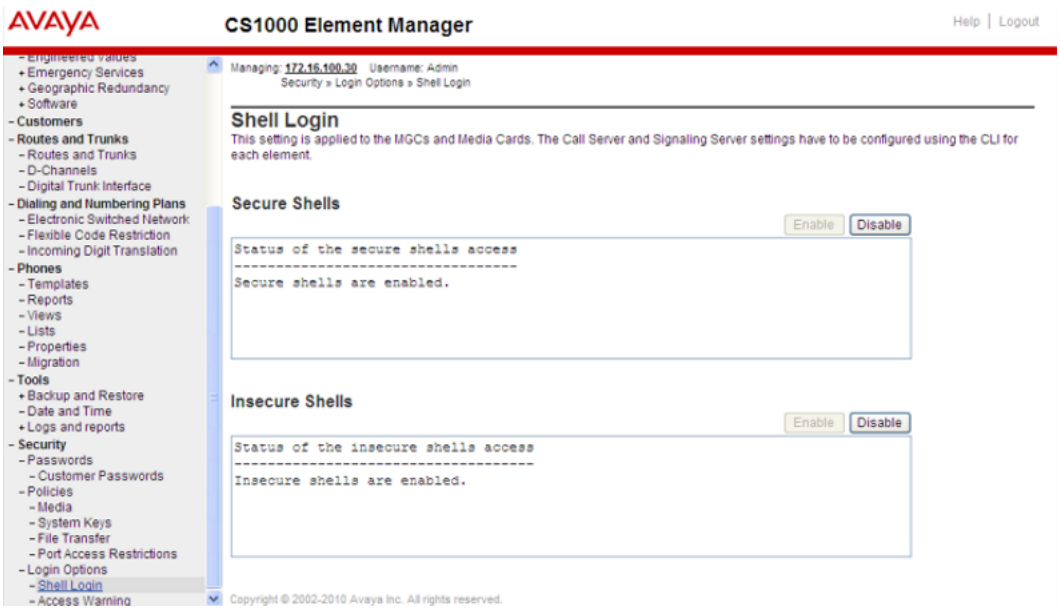
Enable or disable shell access using Element Manager

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.

Enabling or disabling shell access using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click Security > Login Options > Shell Login.

   The status of secure shell access appears in the Secure Shells pane.



3. Click **Enable** or **Disable** to activate or deactivate Secure Shells or Insecure Shells.

Access the system remotely

SSH, a secure form of rlogin, provides a secure method of logging on remotely. The number of active remote logon shells, including rlogin and SSH sessions, cannot exceed 16 sessions on a system.

To log on remotely using SSH, you must have an SSH client installed on your local system. If your local system runs Microsoft Windows, several SSH clients are available; consult your system administrator to find out what SSH client is installed, and how to use it to log on remotely.

Use the following procedure if your local system runs a UNIX-like operating system (for instance, Linux).

Log on remotely with SSH using CLI

1. Access the command line interface (CLI) of your operating system.
2. At the operating system command prompt, enter `$ ssh -l <username> <remote_device_IP>`

   A prompt appears requesting a password.
3. Enter the password associated with the user name you entered in the previous step.

Table 62: Variable definitions

Variable	Value
<username>	A valid user name on the remote device to which you want to log on.
<remote_device_IP>	The IP of the remote device to which you want to log on.

SSH key synchronization between active and inactive cores

To support the joining of standby (inactive) cores to the Unified Communications Management security domain, SSH keys are synchronized between active and inactive cores in redundant systems. The same IP address and SSH key is used for the redundant system, regardless of the core that is active.

Manage SSH keys using overlays

Use the procedures in this section to generate, activate, view, or clear SSH keys using overlays.

Use the following procedure to generate SSH keys from the Call Server.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Generating SSH keys by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 prompt, enter `SSH KEY GENERATE {ACTIVE|INACTIVE|CABINET [n]}`
   For more information about the arguments for this command, see Table 63: Job aid: arguments for SSH KEY GENERATE on page 270.

   When you generate a key, the mutual trust between the device and the Unified Communications Management primary security server is broken until the device rejoins the security domain. A warning message prompts you to do this.

Table 63: Job aid: arguments for SSH KEY GENERATE

Command argument	Purpose
`SSH KEY GENERATE`	Generates the active SSH keys in the active core. After the key generation, the key is synchronized with the inactive core.
`SSH KEY GENERATE ACTIVE`	Generates the active SSH keys in the active core. After the key generation, the key is synchronized with the inactive core.

Table continues…

Command argument	Purpose
SSH KEY GENERATE INACTIVE	Generates the active SSH keys in the inactive core. After the key generation, the key is synchronized with the active core.
SSH KEY GENERATE CABINET [n]	Generates 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 view SSH keys from the Call Server.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Viewing SSH keys by using LD 117

1. Log on to the Call Server CLI.
2. At the LD 117 prompt, enter SSH KEY SHOW {ACTIVE|INACTIVE|CABINET [n]} For more information about the arguments for this command, see Table 64: Job aid: arguments for SSH KEY SHOW on page 271.

Table 64: Job aid: arguments for SSH KEY SHOW

Command argument	Purpose
SSH KEY SHOW	To display the SSH key fingerprint for the active (ENBL) and inactive (STDBY) cores.
SSH KEY SHOW ACTIVE	To display the SSH key fingerprint for the active (ENBL) core.
SSH KEY SHOW INACTIVE	To display the SSH key fingerprint for the inactive (STDBY) core.

Use the following procedure to clear SSH keys from the Call Server. You must disable secure shells before you can clear SSH keys. For the procedure to disable secure shells, see Managing secure shell access by using LD 117 on page 266.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing Enter.

Clearing SSH keys by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 prompt, enter SSH KEY CLEAR {ACTIVE|INACTIVE|CABINET [n]} For more information about the arguments for this command, see Table 65: Job aid: arguments for SSH KEY CLEAR on page 271.

Table 65: Job aid: arguments for SSH KEY CLEAR

Command argument	Purpose
SSH KEY CLEAR	To clear SSH keys stored in the active and inactive cores.
SSH KEY CLEAR ACTIVE	To clear the SSH key for the active core. The SSH key stored in the inactive core is removed during the key synchronization process.

Table continues…

Command argument	Purpose
`SSH KEY CLEAR INACTIVE`	To clear the SSH key for the inactive core. The SSH key stored in the active core is removed during the key synchronization process.
`SSH KEY CLEAR CABINET [n]`	To clear all of the public keys (active as well as pending) stored on the expansion cabinet or MG1000E system. The variable [n] identifies the cabinet, and can be a number, or the keyword ALL.

Manage SSH keys using CLI

Use the procedures in this section to generate, view, or clear SSH keys from the OAM, PDT, or IPL prompt.

Use the following procedure to generate SSH keys by using CLI.

Generating SSH keys by using OAM, PDT, or IPL

1. Log on to the Call Server CLI using a PDT2 account.
2. At the OAM, PDT, or IPL prompt, enter `SSH KEY GENERATE` to generate the key on the Call Server, Gateway Controller, or Voice Gateway Media Card.

Use the following procedure to view SSH keys by using CLI.

Viewing SSH keys by using OAM, PDT, or IPL

1. Log on to the Call Server CLI.
2. At the OAM, PDT, or IPL prompt, enter `SSH KEY SHOW` to display the fingerprint of the public key of the Call Server, Gateway Controller, or Voice Gateway Media Card. Displays both active and pending keys.

Use the following procedure to clear SSH keys by using CLI.

Prerequisites

- You must disable secure shells before you can clear SSH keys.

Clearing SSH keys by using OAM, PDT, or IPL

1. Log on to the Call Server CLI using a PDT2 account.
2. At the OAM, PDT, or IPL prompt, enter `SSH KEY CLEAR` to clear all of the public keys (active as well as pending) stored on the Call Server, Gateway Controller, or Voice Gateway Media Card.

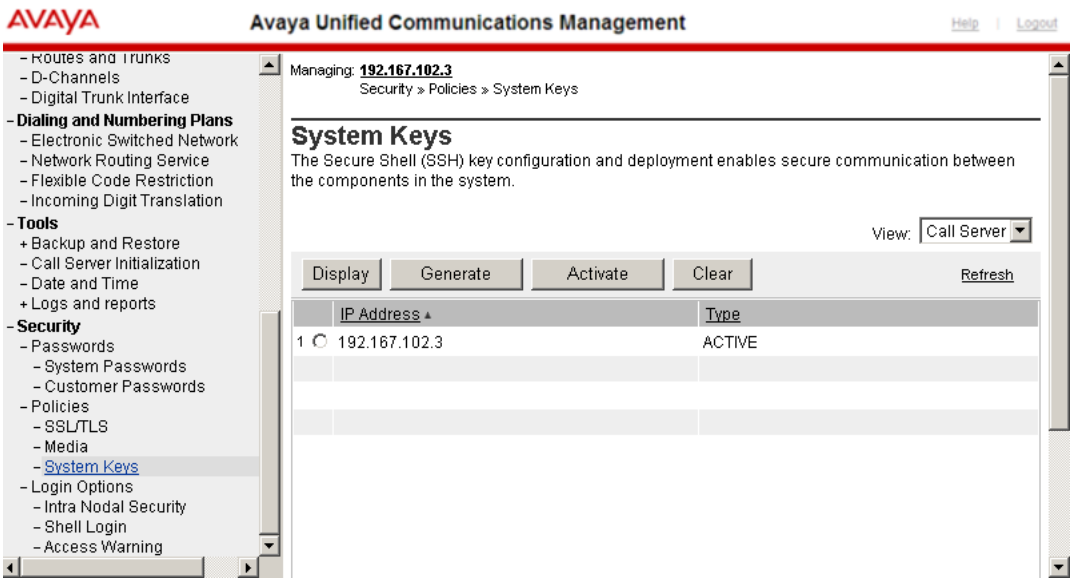
SSH key management using Element Manager

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

Managing SSH keys by using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click Security > Policies > System Keys .

   The System Keys page appears.



3. Use the **View** list to select one of:

   - **Call Server**
   - **IPMG**
   - **SS/Voice Gateway Media Card**

   The data table displays a list of existing keys in the category you selected. You can sort the columns in the data table by clicking on the column heading.
4. Select the radio button next to the entry you want to edit or view.
5. Either:

   Click **Display** The System Key fingerprint information is appears the System Response pane.

   OR

   Click **Clear** The System key information is cleared, and the system response appears in the System Response pane.

   OR

   Click **Generate** The System key information is generated, and the system response appears in the System Response pane.

   OR

   Click **Activate** The System key information is activated, and the system response appears in the System Response pane.

Customize the logon banner

The following restrictions apply to the contents of the banner.txt file:

- The file must have the string banner.txt on the first line of the file.
- The file can contain up to 20 lines of text, with up to 80 characters per line.
- The banner text must contain only the following characters: a-z, A-Z, 0-9,,<.>/?;: [{]} ~!@#$ %^&*()_-+=| b).

Manage the custom banner using overlays

Use the procedures in this section to view or change the logon banner, or restore the default logon banner using LD 17.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Viewing the banner by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 `=>` prompt, enter `BANNER SHOW`.

   The current banner text appears.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Loading a new banner by using LD 117

1. Using a program that allows you to send and receive files, log on to the Call Server using a PDT account.
2. Download the file *banner.txt* from the directory `/u/pub/` on the Call Server.
3. Using an ASCII text editor, open the *banner.txt* file that you downloaded in the previous step.
4. Edit the text in the file.
5. Save the file as *banner.txt* in the `/u/pub/` directory on the Call Server.
6. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
7. At the LD 117 `=>` prompt, enter `BANNER LOAD`.

   The contents of the new banner file are loaded.

These changes are distributed to all Voice Gateway Media Card, Gateway Controller and Media Gateway 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 on page 275.

Use the following procedure to restore the default text to the logon banner. Table 11: Default text of the customizable logon banner on page 48 shows the default text.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Restoring the default banner by using LD 117

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 117 `=>` prompt, enter `BANNER RESET`.

   The default logon banner text is restored.

These changes are distributed to all Voice Gateway Media Card, Gateway Controller and Media Gateway devices the next time an EDD takes place, usually within 24 hours. To force an immediate EDD, see Force an EDD using overlays on page 275.

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.

Viewing or editing the custom banner text by using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click **Security > Login Options > Access Warning** .

   The Access Warning page appears.
3. Click **Edit**.

   The Edit Login Banner page appears.
4. Edit the banner text.
5. Click **Save** to save and distribute the new banner file. A confirmation dialog box appears.
6. Click **OK** to save and distribute the banner file.

Use the following procedure to restore the default text to the logon banner. Table 11: Default text of the customizable logon banner on page 48 shows the default text.

Restoring the default banner by using Element Manager

1. Log on to Element Manager using a System password level 2 account.
2. Click **Security > Login Options > Access Warning** .

   The Access Warning page appears.
3. Click **Edit**.

   The Edit Login Banner page appears.
4. Click **Reset**.

Force an EDD using overlays

Many configuration changes on the system do not take effect until an Equipment Data Dump (EDD) occurs. Use the following procedure to cause the system to perform an immediate EDD, which

propagates system changes to all attached devices. An automatic EDD normally occurs at virtual midnight.

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Forcing an EDD by using LD 43

1. Log on to the Call Server CLI using a PWD2 account.
2. At the LD 43 prompt, enter `EDD`. The banner is updated on all peripheral devices (Signaling Server, IPMG, Voice Gateway Media Card, and Inactive Core).

Important:

System changes and files such as those related to account information and the logon banner are also distributed to all attached devices whenever the system is restarted.

Chapter 12: Security debugging

This chapter provides information and procedures to help you perform debugging of security features.

Debug tools are not required during normal operation of the Avaya Communication Server 1000 (Avaya 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 Account Administrator privilege. When enabling debug mode, you can enable it only on specified terminals, which leaves the rest of the terminals in the system secure. Further, the debug mode is turned off after a configurable period of time.

Enable or disable Media Security debug mode

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Enabling Media Security debug mode by using LD 80

1. Log on to the Call Server CLI using a PWD2 account that has ACCT=YES.
2. At the LD 80 prompt, enter **`EMSD <user-name> <time-out>`** to grant the specified user access to the Media Security debug mode for terminals, nodes, and bandwidth management zones.

   For more information about the arguments for this command, see Table 66: Job aid: arguments for the EMSD command on page 278.

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.

Table 66: Job aid: arguments for the EMSD command

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

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Disabling Media Security debug mode by using LD 80

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the LD 80 prompt, enter **CMSD**.

View information about Media Security debug

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

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

Viewing information about Media Security debug mode by using LD 80

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the LD 80 prompt, enter **PMSD**.

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

The following procedure refers to specific prompts; if a prompt appears that is not mentioned in the procedure, you can often bypass it by pressing `Enter`.

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

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

Use Media Security Debug

Media Security debug mode offers two modes of operation, as described in the following table.

Table 67: Media Security debug modes of operation

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

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

- secDebugOverrideEnable
- secDebugOverrideDisable
- secDebugEnable
- secDebugDisable

To get help for any of these commands, enter them without arguments at the PDT prompt. For more information about how to enable or disable Media Security debug mode, see Media Security override in Debug mode for specific terminals on page 280.

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.

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

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. Access the PDT prompt by holding down the **ctrl** key, and typing **pdt**. The PDT prompt appears.
3. At the PDT prompt, enter either:

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

   OR

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

   OR

   secDebugOverrideEnable node <node_range_start> <node_range_end>

   OR

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

Table 68: Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to enable debug mode.
<node_range_start> <node_range_end>	The range of nodes for which to enable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to enable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to enable debug mode.

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

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the PDT2 prompt, enter either:

secDebugOverrideDisable tn <TN_range_start> <TN_range_end>

OR

secDebugOverrideDisable dn <DN_range_start> <DN_range_end>

OR

secDebugOverrideDisable node <node_range_start> <node_range_end>

OR

secDebugOverrideDisable zone <zone_range_start> <zone_range_end>

Table 69: Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to disable debug mode.
<node_range_start> <node_range_end>	The range of nodes for which to disable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to disable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to disable debug mode.

Media Security enabled in Debug Mode for specific terminals

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

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

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

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

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the PDT2 prompt, enter either:

   secDebugEnable tn <TN_range_start> <TN_range_end> [mode]

   OR

   secDebugEnable dn <DN_range_start> <DN_range_end> [mode]

OR

secDebugEnable node <node_range_start> <node_range_end> [mode]

OR

secDebugEnable zone <zone_range_start> <zone_range_end> [mode]

Table 70: Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to enable debug mode.
[mode]	
<node_range_start> <node_range_end>	The range of nodes for which to enable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to enable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to enable debug mode.

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

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the PDT2 prompt, enter either:

   secDebugDisable tn <TN_range_start> <TN_range_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 71: Variable definitions on page 282.

Table 71: Variable definitions

Variable	Value
<DN_range_start> <DN_range_end>	The range of DNs for which to disable debug mode.

Table continues…

Variable	Value
<node_range_start> <node_range_end>	The range of nodes for which to disable debug mode.
<time-out>	The time until the debug mode is disabled, and normal Media Security operation resumes. Configurable in intervals of one minute from 00 00 to 240 00 hours (10 days), in the format XXX YY, where XXX = hours, and YY = minutes.
<TN_range_start> <TN_range_end>	The range of TNs for which to disable debug mode.
<zone_range_start> <zone_range_end>	The range of zones for which to disable debug mode.

View information about Media Security Debug

Use the following procedure to view the following information:

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

Viewing information about Media Security debug by using CLI

1. Log on to the Call Server CLI using an account that has PDT2 privilege.
2. At the PDT2 prompt, enter **`secDebugPrintAll`**.

ISSS debug tools

Use the information in this section to debug ISSS. To reset an ISSS configuration, type isssReset. For more information about CLI commands, see *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

Important:

If ISSS is enabled and active and you plan to remove a Communication Server 1000 system element, you must first decommission ISSS on the device before you can reinstall the device elsewhere.

Prerequisites

- Must be logged on to an account with PWD2 and PDT2 privileges.

Decommissioning ISSS settings locally by using CLI

Use the following procedure to decommission ISSS settings locally on a Voice Gateway Media Card, Media Gateway Controller, or Signaling Server.

1. Log on to the OAM, PDT, or IPL CLI of the device you want to decommission.
2. Type `isssDecom`.
3. At the confirmation prompt, type `yes` to remove all ISSS related configuration information from files and memory locally and shut down all related tasks.

Viewing the ISSS profile information by using CLI

Use the following procedure to view information about ISSS using the OAM, PDT, or IPL prompt.

Important:

Only use the following procedure if ISSS has been enabled on the element for at least 10-30 seconds. Otherwise, an error may occur.

1. Log on to the OAM, PDT, or IPL CLI of the device you want to view information about.
2. Enter `isssShow`.

   All ISSS information appears.

Chapter 13: Security logs and alarms

This chapter provides information about operational measurements (OM), logs, alarms, and diagnostic features.

For information about messages, logs, and alarms, including System Report (SRPTxxxx) messages, Security Alarms (SECAxxxx), and Security Notification Monitor (SECxxxx) messages, see *Avaya 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

Traffic measurements are part of the IP Traffic Report (report 16) and are used to track progress of calls that use Media Security. The following items are tracked:

- calls completed with Media Security <ccms>
- calls completed without Media Security <ccnms>
- calls failed by near end policy <cfnp>
- calls failed by incoming release <cffr>
- outgoing calls switched to RTP <cosr>
- incoming call switched to RTP <cisr>
- calls failed due to lack of resources (not enough Digital Signal Processors (DSP) capable of Secure Real-Time Protocol (SRTP) communication) <cfnr>

You can access these traffic measurements using the **`invs 16`** command, in LD 2, as shown in Table 72: LD 2: Using invs 16 to access OMs on page 286.

Table 72: LD 2: Using invs 16 to access OMs

Prompt	Response	Description
.	invs 16	Print expanded Media Security IP Statistics traffic report 16
OUTPUT		
zone 1 Intrazone	<cmi><cbi><pi><ai><vi><cmip><cul><cupl> <cuj><cur><cuerl><cwl><cwj><cwpl><cwr><cwerl> <ccms><ccnms><cfnp><cffr><cosr><cisr><cfnr>	
Interzone	<cmo><cbo><po><ao><vo><cmip><cul><cupl> <cuj><cur><cuerl><cwl><cwj><cwpl><cwr><cwerl> <ccms><ccnms><cfnp><cffr><cosr><cisr><cfnr>	

Media Security OMs on Signaling Server

The Signaling Server Session Initiation Protocol (SIP) Gateway key management application maintains the Media Security Operational Measurements (OM) listed in Table 73: Media Security OMs on page 286

Table 73: Media Security OMs

OM	Description
SIPVtrkInMSecCallAttempt	Number of secure call origination attempts
SIPVtrkInMSecCallComp	Number of secure call termination attempts
SIPVtrkInMSecErr	Number of secure call originations that have an error in forming the Session Description Protocol (SDP)
SIPVtrkOutMSecCallAttempt	Number of secure call originations completed
SIPVtrkOutMSecCallComp	Number of secure call terminations completed
SIPVtrkOutMSecErr	Number of incoming calls that have incorrect cryptography parameter in the SDP
SIPVtrkMSecCertAuthErr	Number of the certificate authentication failure for Media Security key management

OAM Security OMs

Use the information in this section to access operations, administration, and maintenance (OAM) Security OMs.

Default password change warning

When the default password change warning message appears, the system generates a SEC0029 message to record the event of the warning message, and records it in a log file (/u/rpt/rpt.log) and in a Simple Network Management Protocol (SNMP) trap.

Warning message for Force Password Change

When the default password change warning message appears, the system generates an SRPT195 message to record the event of the warning message, and records the message in a log file (/u/rpt/rpt.log) and in an SNMP trap.

The format of the SRPT195 message is as follows:

```
SRPT195 Force Password Change Activated
```

Example

The following example shows the SRPT195 event log.

```
pdt> rdtail
RPT: ...rd : 95 new reports arrived since last command
RPT: ...rd : showing 16 records up to the newest record
(rec 435)
...
435 :(1/4/04 16:13:13.570) SRPT195 FORCE PASSWORD
CHANGE ACTIVATED
```

TLS logs and alarms

Table 74: SIP TLS OMs on page 287 shows the operational measurements (OMs) relating to Transport Layer Security for Session Initiation Protocol (SIP TLS) that are logged by the SIP Gateway.

Table 74: SIP TLS OMs

OM	Description
SIPVtrkTlsAuthentication Failure	Number of failed authentication attempts
SIPVtrkTlsIncomingAttempt	Number of incoming SIP TLS connection attempts
SIPVtrkTlsIncomingComp	Number of incoming SIP TLS connection attempts that succeeded

Table continues…

OM	Description
SIPVtrkTlsIncomingFailure	Number of incoming SIP TLS connections that failed
SIPVtrkTlsOutgoingAttempt	Number of outgoing SIP TLS connection attempts
SIPVtrkTlsOutgoingComp	Number of outgoing SIP TLS connection attempts that succeeded
SIPVtrkTlsOutgoingFailure	Number of outgoing SIP TLS connections that failed

Element Manager logs the following OMs related to SIP TLS management:

- change of Secure Socket Layer (SSL) or TLS port number
- change in SSL/TLS Usage setting
- change in Accept Self-Signed Server Certificate setting
- change in Require Client Certificate setting
- change in Allow Redirection from SIPS to SIP setting

Table 75: SIP TLS alarms on page 288 shows the alarms relating to TLS that appear on the Signaling Server console as ERROR system logs (syslogs).

Table 75: SIP TLS alarms

Alarm	Description
ITG0113	This alarm indicates a SIP Gateway (GW) TLS initialization failure (severity level: major). This covers conditions such as a failure to read TLS parameters from the configuration file, certificate not found, or certificate invalid.
SEC0001	This alarm indicates that the number of SIP GW TLS connection failures for a remote IP exceeded the threshold (severity level: major). The initial value of the threshold is 3 failures within 30 minutes from the same remote IP address. The cause of the last failure is indicated in the reason code.

Every day at virtual midnight, the system checks for impending certificate expiry. If any certificate in the system is within 21 days of expiration, the system generates the following alarm: `Certificate to expire within x days (severity level: major) .`

The system generates a log, and optional alarm, whenever any of the following events occur:

- turn SSL ON or OFF
- import certificates
- assign certificates
- delete certificates
- renew existing certificates
- create a new certificate

sFTP security alarms

Table 76: Security alarms related to sFTP on page 289 shows alarms related to Secure File Transport Protocol.

Table 76: Security alarms related to sFTP

Alarm	Description
SEC0087	Secure transfers are enabled. Applications can transfer data based on secure transfer protocols, such as sFTP. This is an informational message; no action is required.
SEC0088	Secure transfers are disabled. Applications cannot transfer data based on secure transfer protocols, such as sFTP. This is an informational message; no action is required.
SEC0089	Insecure transfers are enabled. Applications can transfer data based on insecure transfer protocols, such as FTP. This is an informational message; no action is required.
SEC0090	Insecure transfers are disabled. Applications cannot transfer data based on insecure transfer protocols, such as FTP. This is an informational message; no action is required.

OAM Transaction Audit and Security Event logging

Security audit logs must contain sufficient information for after-the-fact investigation or analysis of security incidents. These audit logs provide a means for accomplishing several security-related objectives including individual accountability, reconstruction of past events, intrusion detection, and problem analysis.

The OAM Transaction Audit Logging feature on Avaya Communication Server 1000 (Avaya CS 1000) maintains an audit trail of all system administrator OAM activities that have taken place on Unified Communications Management User Interfaces. This feature provides the OAM logs only for Avaya CS 1000 management applications running on a Linux platform. The OAM log records include operational, configuration and maintenance events of Communication Server 1000 management applications.

For more information about OAM Transaction Audit logging, see the Communication Server 1000 logging section of *Avaya System Management Reference, NN43001-600*.

Security Event log

The security.log file is stored in the “/var/log/avaya/OAM” directory of the Unified Communications Management Primary Security server. OAM Transaction Audit and Security Event Logging consolidates all Communication Server 1000 security events into security.log. This log file contains

all of the security-related events generated by Communication Server 1000 management applications installed on Linux platforms. These audit log files have a log rotation of 30 days.

Examples of security-related events include:

- Security policy changes
- Logon success and failures
- Certificate changes
- User Account Creation and Illegal (failed) Login Events
- Any OAM security event where security administrator privilege (or flag) is enabled or required

Security administrators can view the security logs by accessing the log viewer interface, which is found by navigating to **Tools > Logs** on the Unified Communications Management primary security server.

For more information about Security Event logging, see the Communication Server 1000 logging section of *Avaya System Management Reference, NN43001-600*.

Appendix A: Standards

This appendix provides information about the Communication Server 1000 system compliance with various security standards. The appendix is divided into the following sections:

Media Security FIPS conformance

The Media Security feature conforms to FIPS 140-2 cryptographic standard Security Level 2. A government and industry working group composed of both operators and vendors developed the FIPS 140-2 standard. The FIPS 140-2 standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. The FIPS 140-2 standard specifies four security levels for cryptographic modules, which provides a wide spectrum of options according to data sensitivity. The Media Security feature conforms to Level 2. Security Level 1 and 2 are described as follows:

- Security Level 1 is the lowest level of security for a cryptographic module. It permits the operations of the software and firmware components on a general purpose computing system using an unevaluated operating system. The operating system is not required to have physical security mechanisms beyond the basic requirements for production grade components, but must have at least one approved algorithm or approved security function.
- Security Level 2 enhances the physical security mechanisms of Security Level 1 by adding requirements for tamper-evidence, which includes the use of temper-evident coating or seals or for pick-resistant locks on removable covers or doors of the module.

  Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform the corresponding services.

  Security Level 2 permits the operation of the software components of the cryptographic module on a general purpose computing system. The operating system must meet the functional requirements specified in the Common Criteria (CC) Protection Profiles (PP), Annex B of FIPS 140-2 specification. The operating system must be evaluated at the CC evaluation assurance level EAL2 (or higher).

Encryption technology

Table 77: Encryption technologies used in CS 1000 on page 292 lists encryption technologies used in Communication Server 1000.

Table 77: Encryption technologies used in CS 1000

Technology	Description
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. SHA-256 is used by SIP TLS (SIP security for SIP Lines and SIP trunks). It is also supported by UNIStim DTLS starting with Release 7.6 SP5. However it is not applicable for Intra System Signaling Security (ISSS).

Note:

Release 7.6 SP5 onwards, Certificate Authority management supports generation of certificates signed with SHA-256 encryption.

When CS 1000 Linux server is deployed as the Primary UCM, you need to provide Private Certificate fields, including bit-length. From Release 7.6 onwards, the Security Configuration view will show a default bit length of 2048, but, 1024 bit length is also available.

Restrictions and limitations for using SHA–256

- Only SHA1 is supported when UCM is installed. SHA–256 is available only after applying the update.
- All the member servers that had joined before applying the update still use the signature algorithm they used while joining.
- For SHA–256 support from the moment of Primary UCM server deployment, you should apply the appropriate update before actual deployment. Go to Local Administration, apply all the required updates in the defined order, then proceed to Full Security Configuration and perform Primary UCM server deployment.

Encryption technology supported in UNIStim DTLS

UNIStim DTLS uses the Mocana DTLS library stack, which is FIPS certified (FIPS 140-2, Level 1, certificate number #927).

The table below lists the ciphers supported by the Mocana DTLS library for UNIStim DTLS in Communication Server 1000 Release 6.0 and later.

Table 78: Ciphers supported by Mocana DTLS library in CS 1000

TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

Appendix B: Check security domain status and registration activity

This section describes commands that you can use to check the status of the security domain and monitor registration activity.

You can view the UCM security server log file in the `/var/log/Nortel/Jboss-Quantum/log` directory to monitor registration activity. To view the latest entries in the log, at the prompt enter:

```
tail -f server.log
```

On the Call Server, you can view the date/time of token creation or distribution by using the PDT/LDB shell and listing the `/e/sdm` directory. The date/time should match what is shown on the UCM security server.

To have all elements join a security domain successfully, each element must be uniquely identified and have an individual SSH key. To verify if this is the case for a particular element, you can view the **baseOS** properties file and verify that the field **elementID** contains the specific FQDN of that element. If the **elementID** entry is similar to **elementId=localhost.localdomain**, then you must change it.

If SSH keys must be cleared and regenerated, see the procedures in Manage SSH keys using overlays on page 270.

The following list describes Call Server and MGC SSH debug commands:

Warning:

These commands should be used with caution as the output is very large and processor-intensive. Do not leave these commands running unattended.

- FCDebug=1
- sshDebug=1
- sshClientDebug=1
- SSHClientDebug=1
- <command>= 0 disables the given debug command.

Appendix C: CS 1000 UCM SHA256 support

With SHA256 update applied, all the newly generated x509 certificates are signed with the latest SHA256 algorithm. SHA256 is included from Release 7.6, Service Pack 5 onwards. You can force switch back to SHA1 for the whole system using the **defaultSAconfig** linux command.

For customers with all system elements on Release 7.6

In some networks, it is critical to have all the certificates, for all elements, signed with SHA256. In this case, the Primary UCM server must be reinstalled, since its Default certificate can only be generated on installation. Following this, Service Pack 5 or higher must be applied before configuring the server as Primary. Finally, rejoin all the elements to the Security Domain.

Note:

During backup or restore, the backup or restore procedure backs up the certificates. Therefore, restoring backup with SHA1 on the SHA256 server will roll back the server to SHA1.

However, in the following cases, you can apply the SHA256 Update without reinstalling Primary UCM server:

- when you want the Default certificate for the Primary UCM signed with SHA1 or when which signature algorithm is used is not important.
- when the reinstallation of Primary UCM server is unacceptable.

In both these cases, the Primary UCM server SHA256 update application does not require any special procedure for x509 certificates. You only need to follow the installation instructions. The Primary will still use the SHA1 Default certificate. Elements requesting SHA256 certificates will get SHA256-signed certificates after rejoining the Security Domain.

When it is necessary to use SHA1 for the whole system, refer the following section.

For customers with mixed releases systems (7.5, 7.0 or lower)

Before installing Service Pack 5 on Primary UCM server, note that:

- After installing SP5 on Primary UCM server, all the newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA256 algorithm.
- To avoid CS1000 systems negotiation breakage, SHA1 certificate must be generated. You can use the Linux command **defaultSAconfig** on the Primary UCM server under user admin2 to change back to SHA1

  After this, all newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA1 algorithm.

- With the help of the same **`defaultSAconfig`** command, the Signature Algorithm can be changed to SHA256 again.

Glossary

Related Links

authentication A process that checks the credentials of a security principal against values in an identity store.

Related Links
Glossary on page 297

authorization

The process of resolving a user's entitlements with the permissions configured on a resource to control access.

Related Links
Glossary on page 297

certificate

In order to verify the identity of an endpoint, some features of the Communication Server 1000 system use a digital certificate.

Related Links
Glossary on page 297

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.

Related Links
Glossary on page 297

EDD

Equipment Data Dump. An EDD propagates system changes to all attached devices. Many configuration changes on the system do not take effect until an EDD takes place. An EDD normally occurs automatically at virtual midnight.

Related Links
Glossary on page 297

fingerprint

In public-key cryptography, a public key fingerprint is used to verify identity.

Related Links
Glossary on page 297

IPsec

The IP Security (IPsec) framework provides intranodal security on the Communication Server 1000 system. IPsec is a standard that can be used to secure internet protocol (IP) communications by encrypting and authenticating IP packets. IPsec provides security at the network layer, and consists of a group of cryptographic protocols for securing packet flows and key exchange. The two packet flows are:

- Encapsulating Security Payload (ESP), which provides authentication, data confidentiality, and message integrity
- Authentication Header (AH), which provides authentication and message integrity, but does not provide confidentiality

IPsec uses the Internet Key Exchange (IKE) protocol.

IPsec operates at Layer 3 (the network layer) of the OSI model. Therefore, IPsec can protect both TCP and UDP-based protocols.

Related Links
Glossary on page 297

LD

(Also Load, Overlay). See Overlay.

Related Links
Glossary on page 297

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.

Related Links
Glossary on page 297

MGC

Media Gateway Controller.

Related Links
Glossary on page 297

MIKEY

In cryptography, a key management protocol.

Related Links
Glossary on page 297

NRS Manager

Network Routing Service Manager. The Network Routing Service (NRS) Manager is a Web interface that you can use to manage the NRS. The NRS Manager application resides on the Signaling Server. The NRS includes both the H.323 Gatekeeper and Session Initiation Protocol (SIP) Redirect/Registrar Server, and provides routing services to both H.323- and SIP-compliant devices.

Related Links
Glossary on page 297

OAM

(Also OA&M). Operation, Administration, and Management.

Related Links
Glossary on page 297

OM

An operational measurement report where information about system activity is stored.

Related Links
Glossary on page 297

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.

Related Links
Glossary on page 297

PEM

Privacy-Enhanced Electronic Mail (PEM) is a proposed Internet Engineering Task Force (IETF) standard that provides cryptographic protection of e-mail messages.

Related Links
Glossary on page 297

SDesc

Security Descriptions

Related Links
Glossary on page 297

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.

Related Links
Glossary on page 297

SFTP

Secure File Transfer Protocol. A network protocol that enables the secure exchange of data using SSH standards. See also the entry for SSH.

Related Links
Glossary on page 297

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).

Related Links
Glossary on page 297

SIP

Session Initiation Protocol (SIP) is a protocol for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. SIP clients traditionally use TCP and UDP port 5060 to connect to SIP endpoints, including SIP servers. Telephony systems use SIP in setting up and tearing down voice or video calls. However, SIP also offers session initiation for applications such as Event Subscription and Notification, Terminal mobility. All voice and video communications are transmitted using Real-time Transport Protocol (RTP).

Related Links

Glossary on page 297

SRTP

Secure Real-time Transport Protocol (or SRTP) is a secure form of Real-time Transport Protocol (RTP). SRTP provides encryption, authentication, and replay protection, and protects message integrity for RTP data in both unicast and multicast applications. A related protocol, Secure RTCP (SRTCP), provides the same security-related features to RTCP that SRTP provides to RTP.

Related Links

Glossary on page 297

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 .

Related Links

Glossary on page 297

TDM

Time Division Multiplexing.

Related Links

Glossary on page 297

TLS

Transport Layer Security (TLS), (which replaces Secure Socket Layer [SSL]) is a cryptographic protocol that provides secure communications over the Internet for applications such as e-mail, Internet fax, and other data transfers that require security. In many applications, only the server is authenticated, and the client is unauthenticated. TLS also supports mutual authentication, which requires that a public key infrastructure be deployed to the clients. In either case, TLS protects communication from eavesdropping, tampering, and message forgery.

Related Links

Glossary on page 297

TN

Terminal Number.

Related Links

Glossary on page 297

Index

K

L

M

N

P

R

S

T

U

V