



User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6014-02



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

User Guide for CiscoView Device Manager for the Cisco SSL Services Module
Copyright © 2003-2005 Cisco Systems, Inc. All rights reserved.



Preface **xiii**

Audience **xiii**

Conventions **xiii**

Product Documentation **xiv**

Related Documentation **xv**

Obtaining Documentation **xvi**

 Cisco.com **xvi**

 Documentation DVD **xvi**

 Ordering Documentation **xvii**

Documentation Feedback **xvii**

Cisco Product Security Overview **xviii**

 Reporting Security Problems in Cisco Products **xviii**

Obtaining Technical Assistance **xix**

 Cisco Technical Support Website **xix**

 Submitting a Service Request **xx**

 Definitions of Service Request Severity **xxi**

Obtaining Additional Publications and Information **xxi**

CHAPTER 1

Getting Started with CVDM-SSLSM **1-1**

 Before You Begin **1-2**

 What's New **1-3**

 Key Features in CVDM-SSLSM **1-4**

 Starting CVDM-SSLSM **1-5**

 Installing the Java Plug-in **1-5**

- Navigating in CVDM-SSLSM 1-6
 - Understanding the CVDM-SSLSM Desktop 1-7
 - What Does the Home Page Show Me? 1-11
- What Does the Setup Page Show Me? 1-17
 - Selector 1-18
 - Understanding the Action Buttons 1-20
- Editing the Preferences 1-21
- Viewing Running Configuration 1-22
- Delivering CLI Commands to the Device 1-22
- What's Next? 1-24

CHAPTER 2

PKI Overview 2-1

- Public Key Infrastructure 2-1
- Configuring Keys and Certificates 2-2

CHAPTER 3

Managing Certificates 3-1

- Getting started with Wizards 3-2
 - Certificate Wizards 3-2
 - Configuring a Certificate Trustpoint Using the Wizard 3-2
 - Import Certificates and Private Key 3-4
 - Export Certificates and Private Keys 3-7
- Understanding Wizards 3-10
 - Launching Certificate Wizards 3-11
 - Configuring a Certificate Trustpoint Using the Wizard 3-12
 - Setting up a Proxy Service Trustpoint 3-13
 - Setting up a CA Trustpoint 3-14
 - Configuring a Trustpoint and RSA Key Pair 3-15
 - Configuring SSL Certificate Attributes 3-16
 - Configuring Enrollment Parameters 3-17

Selecting a CA Certificate Source	3-19
Importing a CA Certificate Chain	3-20
Importing a CA Certificate Chain from a Local Hard Disk	3-21
Importing a CA Certificate Chain using Copy and Paste	3-22
Importing a CA Certificate Chain from a TFTP Server	3-23
Configuring Trustpoint Tasks	3-24
Viewing Wizard Summary	3-24
Delivering Configuration to an SSL Module	3-25
Viewing Trustpoint Configuration Status	3-25
Viewing Certificate Signing Request (CSR)	3-25
Importing and Exporting Certificates	3-26
Importing Certificates from an External PKI System	3-26
Importing PKCS#12 File	3-26
Importing PEM File	3-27
Configuring Certificate Source and Format	3-28
Specifying Certificates and Private Key	3-32
Specifying CA Certificates	3-34
Configuring Certificates and Key Files (PEM - Local Hard Disk)	3-35
Configuring Certificates and Key Files (PEM - Remote System)	3-36
Specifying a CA Certificate (PEM)	3-37
Specifying Private Key (PEM Format)	3-37
Specifying SSL Certificate (PEM Format)	3-37
Viewing the Summary	3-37
Delivering Configuration to SSL Module	3-38
Viewing the Certificate Import Status	3-38
Exporting Certificates Using the Wizard	3-38
Exporting certificates of more than one Trustpoint	3-38
Exporting certificates of a selected Trustpoint	3-38
Exporting PKCS#12 Files	3-39
Exporting PEM Files	3-40

- Certificate Format and Destination **3-40**
- Certificate and Key Pair Files (PEM - Local Hard Disk) **3-42**
- Certificate and Key Pair Files (PEM - Remote File System) **3-42**
- Viewing Certificate Export Wizard Summary **3-43**
- Viewing the Certificate Export Status **3-43**
- Exporting Certificates in Bulk Using the Certificate Export Wizard **3-44**
 - Selecting Certificates and Format (PEM, PKCS#12) **3-45**
 - Adding Certificates and Trustpoints for exporting **3-46**
 - Specifying the Destination (PEM) **3-47**
 - Specify Destination Details (PEM - Local Hard Disk) **3-48**
 - Specify Destination Details (Copy and Paste) **3-49**
 - Specify Destination Details (PEM - Remote System) **3-49**
 - Specify Destination Details (PEM - Redundant SSLSM) **3-50**
 - Specifying the Destination (PKCS#12) **3-51**
 - Specify Destination Details (PKCS#12 - Remote System) **3-51**
 - Specify Destination Details (PKCS#12 - Redundant SSLSM) **3-52**
- Viewing Certificate Trustpoints **3-54**
 - Certificate Trustpoint Grouper **3-57**
- Certificate Trustpoint Details **3-58**
 - Authenticating Trustpoints **3-65**
 - Enrolling Trustpoints **3-65**
 - Authenticating and Enrolling Trustpoints **3-66**
 - Importing SSL Certificate Trustpoints **3-66**
 - Renewing Trustpoints **3-67**
 - Exporting Trustpoints **3-68**
- Editing Trustpoint Configuration **3-68**
 - Selecting Available ACLs **3-72**
 - Selecting Available Key Pairs **3-72**
- Certificate Hierarchy **3-73**

Deleting Certificates	3-74
Challenge Password	3-75
How Do I...	3-75
How Do I Import an SSL Certificate and Private Key to SSLSM?	3-76
How do I Import a CA Certificate Chain on the SSLSM?	3-77
How do I generate a Certificate Signing Request (CSR)?	3-78
How do I import the SSL certificate obtained using CSR?	3-81
How Do I Export Certificates and Private Keys from SSLSM?	3-82
How Do I Renew an SSL Certificate?	3-82

CHAPTER 4**Managing Key Pairs 4-1**

Understanding Key Pairs	4-1
Viewing Key Pairs	4-2
Adding Key Pairs	4-4
Deleting Key Pairs	4-6
Key Pair Wizard	4-6
Key Pair Import Wizard	4-7
Specify Key Pair Name and Source	4-7
Public and Private Keys (Local Hard Disk)	4-8
Public and Private Keys (Copy-and-Paste)	4-8
Public and Private Keys (Remote System)	4-9
Key Pair Export Wizard	4-10
Key Pair Destination	4-10
Destination Files and Encryption Parameters (Local Hard Disk)	4-11
Encryption Parameters (Copy-and-paste)	4-13
Destination Files and Encryption Parameters (Remote System)	4-14
Key Pair Wizard Summary	4-15
Key Pair Wizard Status	4-15

How Do I... 4-16
 How Do I Add a New Key Pair? 4-16
 How Do I Import a Key Pair? 4-16

CHAPTER 5

Managing CA Pools 5-1
 Viewing CA Pools 5-2
 Assigning CA Pools to Proxy Services 5-4
 Adding CA Pools 5-5
 Editing CA Pools 5-6
 Deleting CA Pools 5-7
 How Do I... 5-7
 How do I add a new CA Pool? 5-7

CHAPTER 6

Managing Certificate ACLs 6-1
 Viewing Certificate ACLs 6-2
 Assigning Certificate ACLs to Trustpoints 6-4
 Viewing Associated Trustpoints 6-5
 Adding Certificate ACL 6-5
 Editing Certificate ACLs 6-7
 Deleting Certificate ACLs 6-9

CHAPTER 7

Managing Proxy Services 7-1
 Proxy Service Wizards 7-2
 Basic Proxy Service Wizard 7-3
 Defining Proxy Service Name and Type 7-4
 Configuring Client Side (Virtual) and Server Parameters 7-5
 Assigning Certificate to Proxy Services 7-6

Selecting Available Certificate Trustpoints	7-7
Viewing Proxy Service Setup Summary	7-7
Advanced Proxy Service Wizard	7-8
Defining Proxy Service Name and Type	7-9
Configuring Client Side (Virtual) and Server Parameters	7-10
Assigning Certificate to Proxy Service	7-11
Assigning Policies to Proxy Services	7-11
Assigning TCP Policy to Proxy Services	7-12
Viewing Advanced Proxy Service Setup Summary	7-13
Selecting Available NAT Pools	7-13
Selecting Available CA Pools	7-14
Viewing Proxy Services	7-15
Viewing Proxy Services Details	7-18
Editing Proxy Service Configuration	7-22
NAT Pools	7-26
Understanding NAT Pools	7-27
Server NAT	7-27
Client NAT	7-27
Viewing NAT Pools	7-28
Adding NAT Pools	7-29
Deleting NAT Pools	7-30
Assigning NAT Pools to Proxy Services	7-30
Selecting Available CA Pools	7-31
Selecting Available NAT Pools	7-31
Selecting Available Certificate Trustpoints	7-32
How Do I...	7-32
How Do I Setup a Proxy Service?	7-32
Troubleshooting Proxy Services	7-33

CHAPTER 8

Managing Policies 8-1

TCP Policy 8-3

Viewing TCP Policies 8-3

Assigning Policies to Proxy Services 8-5

Adding TCP Policy 8-7

Editing TCP Policy 8-8

Deleting TCP Policy 8-10

SSL Policy 8-10

Viewing SSL Policy 8-10

Adding SSL Policies 8-12

Editing SSL Policies 8-14

Deleting SSL Policy 8-16

HTTP Header Insertion Policy 8-17

Viewing HTTP Header Insertion Policy 8-19

Adding HTTP Header Insertion Policy 8-21

Editing HTTP Header Insertion Policy 8-22

Deleting HTTP Header Insertion Policy 8-23

URL Rewrite Policy 8-23

Viewing URL Rewrite Policy 8-24

Adding URL Rewrite Policy 8-26

Editing URL Rewrite Policy 8-27

Viewing URL Rules and Outcome 8-29

Deleting URL Rewrite Policy 8-30

CHAPTER 9

Managing VLANs 9-1

Viewing VLANs 9-2

Adding VLANs 9-3

Editing VLANs 9-4

Deleting VLANs 9-4

CHAPTER 10**Viewing Statistics 10-1**

TCP Statistics 10-2

SSL Statistics 10-4

Proxy SSL Statistics Summary 10-8

Proxy SSL Statistics - Proxy Services 10-10

.Proxy Service SSL Statistics 10-12

PKI Statistics 10-13

INDEX



Preface

This guide describes CiscoView Device Manager for SSL Services Module (CVDM-SSLSM) and describes common tasks you can accomplish with CVDM-SSLSM.

Audience

This document is for the experienced network operator, security operator, or super administrator managing Cisco Catalyst 6500 family of switches.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font

Item	Convention
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)</i>	This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/prod_release_notes_list.html
<i>User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)</i>	This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html
Context-sensitive online help	Click the Help button from any dialog box within the application.

Related Documentation


Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 2](#) describes the additional documentation that is available.

Table 2 **Related Documentation**

Document Title	Available Formats
<i>ReadMe Document for CiscoView Device Manager for Cisco Catalyst 6500 (CVDM-C6500)</i>	<p>This document is available if you download CVDM-C6500 from the software download site. You can reach the CVDM-C6500 download site by clicking the Software Center link from this URL: http://www.cisco.com/go/cvdm</p> <p>Note It is important that you read this document before downloading and installing CVDM-C6500 from the software download site.</p>
<i>Release Notes for CiscoView Device Manager for Cisco Catalyst 6500 (CVDM-C6500)</i>	<p>This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/prod_release_notes_list.html</p>
<i>User Guide for CiscoView Device Manager for Cisco Catalyst 6500</i>	<p>This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html</p>
<i>ReadMe Document for CiscoView Device Manager for Cisco Content Switching Modules (CVDM-CSM)</i>	<p>This document is available if you download CVDM-CSM from the software download site. You can reach the CVDM-CSM download site by clicking the Software Center link from this URL: http://www.cisco.com/go/cvdm</p> <p>Note It is important that you read this document before downloading and installing CVDM-CSM from the software download site.</p>

Table 2 **Related Documentation (continued)**

Document Title	Available Formats
<i>Release Notes for CiscoView Device Manager for Cisco Content Switching Modules (CVDM-CSM)</i>	This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/prod_release_notes_list.html
<i>User Guide for CiscoView Device Manager for Cisco Content Switching Modules (CVDM-CSM)</i>	This document is available on Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and

troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



PART 1

CVDM-SSLSM Basics





Getting Started with CVDM-SSLSM

The CiscoView Device Manager for Cisco Catalyst 6500 SSL Services Module is an embedded device manager for single service module setup, feature and services configuration, and monitoring of the services module.

SSLSM Overview

The Secure Socket Layer Services Module is a Layer 4-through-Layer 7 service module that you can install into the Catalyst 6500 series switch. The module terminates secure socket layer (SSL) transactions and accelerates the encryption and decryption of data used in SSL sessions.

The module operates either in a standalone configuration or with the Content Switching Module (CSM). In a standalone configuration, secure traffic is directed to the module using policy-based routing (PBR). When used with the CSM, only encrypted client traffic is forwarded to the module, while clear text traffic is forwarded to the real servers.

The SSLSM uses the SSL protocol to enable secure transactions of data through privacy, authentication, and data integrity; the protocol relies upon certificates, public keys, and private keys.

The certificates, which are issued by certificate authority and are similar to digital ID cards, verify the identity of the server to the clients and the clients to the server. The certificates include the name of the entity to which the certificate was issued, the public key of the entity, and the time stamp that indicates the certificate expiration date.

The public and private keys are the ciphers that are used to encrypt and decrypt information. The public key is shared without any restrictions, but the private key is never shared. Each public-private key pair works together; data that is encrypted with the public key can only be decrypted with the corresponding private key.

This chapter includes the following topics:

- [Before You Begin, page 1-2](#)
- [What's New, page 1-3](#)
- [Key Features in CVDM-SSLSM, page 1-4](#)
- [Starting CVDM-SSLSM, page 1-5](#)
- [Navigating in CVDM-SSLSM, page 1-6](#)
- [Editing the Preferences, page 1-21](#)
- [What Does the Setup Page Show Me?, page 1-17](#)
- [Viewing Running Configuration, page 1-22](#)
- [Delivering CLI Commands to the Device, page 1-22](#)
- [What's Next?, page 1-24](#)

Before You Begin

Before you begin using CVDM-SSLSM:

- Make sure you have gone through the CVDM-SSLSM Readme and Release Notes.
- Install the necessary Java Plug-in
- Make sure you have necessary privileges. Privilege level 15 is ideal.

What's New

The new features in this release are:

Table 1-1 ***New Features for CVDM-SSLSM 1.1***

Feature	Description
Public Key Infrastructure	<p>New features are:</p> <ul style="list-style-type: none">• Import private key in Netscape Server Key (NET) format and certificates in DER format.• Import unencrypted keys.• Import certificate chain in PEM and PKCS7 format.• Certificate and private key validations.• Bulk export of certificates.• Export certificates to a redundant SSLSM.• Certificate Browser.
Statistics	<ul style="list-style-type: none">• Statistics at proxy service granularity.• Delta monitoring.• Option to reset the counters.• Auto refresh of statistics.

Key Features in CVDM-SSLSM

The following table describes the key features of CVDM-SSLSM:

Table 1-2 **Key Features**

Feature	Description
Public Key Infrastructure	CVDM-SSLSM allows you to: <ul style="list-style-type: none"> • Manage Certificates: <ul style="list-style-type: none"> – Declare Trustpoints, import and export certificates – Visual indication of expiring and missing configured certificates. – Grouping of the Trustpoints by CA, enrollment status, and expiration date. – Certificate Wizards to create and enroll certificates, import and export certificates. • Create and manage Key Pairs • Create and manage ACLs • Create and manage certification authority pools
Proxy Service	CVDM-SSLSM allows you to set up server proxy, client proxy and enable backend encryption service using this feature.
Policies	CVDM-SSLSM allows you configure SSL policy, TCP, header insertion, and URL rewrite policies.
Statistics	CVDM-SSLSM shows you the TCP, SSL, and PKI statistics.

Starting CVDM-SSLSM

-
- Step 1** In your browser, enter the IP address or DNS hostname of the SSLSM. The Enter Network Password dialog box appears.
 - Step 2** Enter your SSLSM username and password.
 - Step 3** Click **OK**. The CVDM splash screen appears.
 - Step 4** Enter your device username and password.
 - Step 5** Click **Yes**. The Warning - Security dialog box appears. To accept the security certificate and continue, click **Yes**.
 - Step 6** The SSH Credentials dialog box appears.
 - Step 7** Enter your SSH username and password. The Enter Enable Password dialog box appears.
 - Step 8** Enter enable password.
 - Step 9** Click **OK**. CVDM-SSLSM homepage appears.
-

Installing the Java Plug-in

You need to install the Java Plug-in. Java Plug-in improves the performance of CVDM-SSLSM and allows the application to use the latest Java runtime functionality. For CVDM, the plug-in speeds up caching and application loading. CVDM-SSLSM requires the Java Plug-in version 1.4.2_04.

The first time you invoke any Java Plug-in window, you are alerted if the plug-in is not installed. CVDM-SSLSM prompts you to download and install the plug-in files, using the installation screens or the procedure displayed. The next time you start the application, CVDM-SSLSM automatically uses the plug-in. Install the Java Plug-in provided with CVDM-SSLSM.

Navigating in CVDM-SSLSM

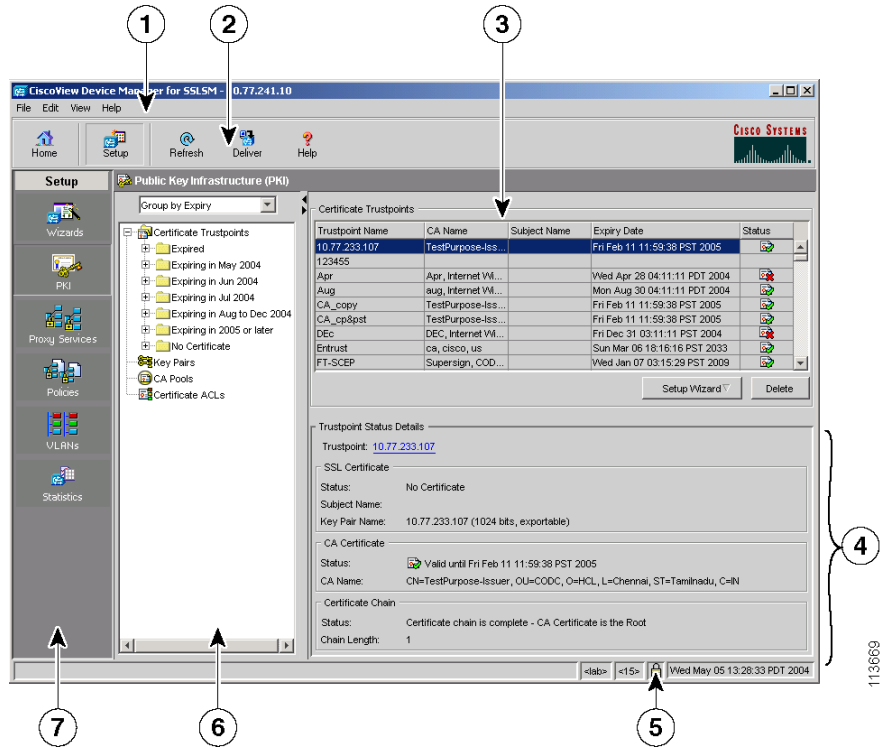
Before you begin using CVDM-SSLSM, you must understand the basic operation of the user interface, including the login procedure and user interface elements. See the following sections for more information:

- [Understanding the CVDM-SSLSM Desktop, page 1-7](#)
- [What Does the Home Page Show Me?, page 1-11](#)
- [What Does the Setup Page Show Me?, page 1-17](#)
- [Understanding the Action Buttons, page 1-20](#)

Understanding the CVDM-SSLSM Desktop

This section describes the main GUI elements of the CVDM-SSLSM application (see [Figure 1-1](#)).

Figure 1-1 CVDM-SSLSM GUI Elements



113669

Figure 1-1 Reference	Location	Description
1	Menu bar	<p>Provides File, Edit, View, and Help options.</p> <ul style="list-style-type: none"> • File <ul style="list-style-type: none"> – File > Save to Startup—Saves the configuration running on the device as the startup configuration. – File > Exit—Logs you out of CVDM-SSLSM and closes the application. A warning appears if any configuration has not been applied to the SSLSM. • Edit <ul style="list-style-type: none"> – Edit > Preferences—Displays the Preferences dialog box, from which you can edit application preferences. For details, see Editing the Preferences, page 1-21 • View <ul style="list-style-type: none"> – View > Home—Displays the Home page. – View > Setup—Displays the Features page. – View > Running Config > SSLSM...—Displays the configuration running on the SSLSM. For details, see Viewing Running Configuration, page 1-22 – View > Refresh—Collects the most recent device information and updates CVDM-SSLSM with it. – View > Transport Log...—Displays the transport log of the device. You can clear the log or save the information to a file. • Help <ul style="list-style-type: none"> – Help > Help Topics—Displays online help. – Help > About—Displays CVDM-SSLSM version information.

Figure 1-1 Reference	Location	Description
2	Task bar	Provides access to CVDM-SSLSM functionality. <ul style="list-style-type: none"> • Home—Displays the home page. • Setup—Displays the features page. • Refresh—Collects the most recent device information and updates CVDM-SSLSM with it. • Deliver—Opens the Deliver Configuration to SSLSM dialog box, from which you can send accumulated CLI commands to the device. For details, see Delivering CLI Commands to the Device, page 1-22 • Help—Displays context-sensitive help.
3	Page	CVDM-SSLSM working area in which you perform tasks.
4	Pane	One part of a divided page or dialog box.
5	Status bar	Provides the following information: <ul style="list-style-type: none"> • Message describing the status of the application. • Application user and privilege level. • Icon showing the security level of the connection. • Time stamp of the application startup time.
6	Selector	Hierarchy of the groups and objects available on the services page that allows you to access specific functions for a service module object. See “Selector” section on page 1-18 for more information.
7	Left-most pane	Contains buttons, on the setup page, that allow you to access SSLSM functions.

What Does the Home Page Show Me?

The home page is the first screen that comes up when you start CVDM-SSLSM. It provides an overview of CVDM-SSLSM (see [Figure 1-2](#)).

Figure 1-2 CVDM-SSLSM Home Page

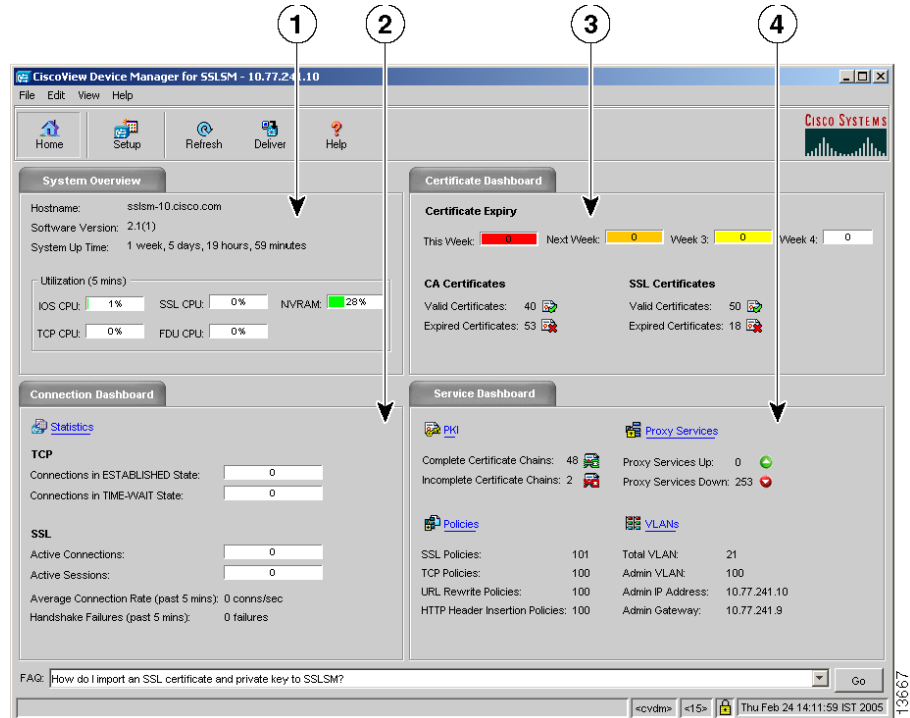


Table 1-3 *CVDM-SSLSM Home Page Elements and Description*

Figure 1-3 Reference	Location	Description
1	System Overview tab	Displays the overview of the system.
2	Connection Dashboard tab	Displays the statistics of the traffic through the SSLSM.
3	Certificate Dashboard tab	Displays the information on the certificates.
4	Service Dashboard tab	Displays the information on the PKI service, proxy service, policies, and VLANs.

The System Overview Dashboard displays the following information:

Field	Description
Hostname	The hostname of the SSLSM.
Software Version	The application image version.

Field	Description
System Up Time	The time elapsed since the SSL module was started.
Utilization (5 mins)	<p data-bbox="803 318 1240 375">System utilization during the last 5 minutes.</p> <p data-bbox="803 396 1224 453">The following utilization information is available:</p> <ul data-bbox="817 474 1233 867" style="list-style-type: none"><li data-bbox="817 474 1233 531">• IOS CPU—The average utilization of the System CPU.<li data-bbox="817 550 1233 607">• TCP CPU—The average utilization of the System CPU.<li data-bbox="817 626 1233 683">• SSL CPU—The average utilization of the System CPU.<li data-bbox="817 703 1233 760">• FDU CPU—The average utilization of the System CPU.<li data-bbox="817 779 1233 867">• NVRAM—NVRAM utilization – [NVRAM size in use / NVRAM size] <p data-bbox="803 888 1233 1010">Note The utilization values are not updated in real time. You need to refresh the application to update the utilization.</p>

The Certificate Dashboard displays the following information:




Certificate Expiry Dashboard	<p>Number of certificates expiring in the near future. The expiry count will be displayed at weekly granularity.</p> <p>This Week Number of certificates that will expire this week.</p> <p>Next Week Number of certificates that will expire next week.</p> <p>Week 3 Number of certificates that will expire the week after next.</p> <p>Week 4 Number of certificates that will expire in the fourth week from now.</p>
CA Certificates	
Valid Certificates	The number of valid CA certificates.
Expired Certificates	The number of invalid CA certificates.
SSL Certificates	
Valid Certificates	The number of valid SSL certificates.
Expired Certificates	The number of invalid SSL certificates.


The Connection Dashboard displays the following information:

Statistics	The statistics are not updated in real time. You can view and update the statistics in Setup > Statistics .
TCP	
Connections in ESTABLISHED state	Number of TCP connections in connections Established state.
Connections in TIME-WAIT state	Number of TCP connections in connections Time-Wait state.

SSL	
Active Sessions	The number of SSL sessions with active connections. The value is rendered as horizontal bar charts.
Active Connections	The number of SSL connections in data, handshake and re-negotiation phase. The value is rendered as horizontal bar charts.
Average Connection Rate (past 5 mins)	The rate at which successful connections were setup in the past 5 minutes.
Handshake Failures (past 5 mins)	Total handshake failures in the past 5 minutes.

The Service Dashboard displays the following information:

PKI	
Complete Certificate Chains	Number of complete certificate chains. A  icon indicates that the certificate chain is complete.
Incomplete Certificate Chains	Number of incomplete certificate chains. A  icon indicates that the certificate chain is incomplete.
Proxy Services	
Proxy Services Up	Total Proxy Services that are operational. A  icon indicates that the module is operationally up.

Proxy Services Down	<p>Proxy services not operational due to fault conditions: invalid certificate, lack of server connectivity, and so forth, and those that are administratively down.</p> <p>A  icon indicates that the module is administratively and operationally down.</p> <p>In Setup > Proxy Services dialog box, the administratively down status and operationally down status is indicated using different icons.</p>
Policies	
SSL Policies	Number of SSL policies configured on the module.
TCP Policies	Number of TCP policies configured on the module.
URL Rewrite Policies	Number of URL rewrite policies configured on the module.
HTTP Header Insertion Policies	Number of HTTP Header Insertion policies configured on the module.
VLANs	
Total VLANs	Number of VLANs on the module.
Admin VLAN	The admin VLAN ID.
Admin IP Address	IP Address of the admin VLAN.
Admin Gateway	IP Address of the gateway configured for the admin VLAN.

All group objects contains a hyperlink. Click on the links to view the details for a group object.

FAQ

You can find answers for your questions on important tasks using FAQ. Select a question from the FAQ list, then click **Go**.

What Does the Setup Page Show Me?

The Setup page allows you to access the CVDM-SSLSM features. You can launch wizards from this page or you can start using the PKI, Proxy Service, Policy and VLAN features.

When you reach the Setup page, the following GUI elements appear in a pane on the left side of the content window:

GUI Element	Description
Wizards	Click to launch wizards that will guide you to in creating and managing Trustpoints and proxy services.
PKI	Allows you to manage public key infrastructure on the SSLSM.
Proxy Services	Allows you to manage SSL proxy services on the SSLSM.
Policies	Allows you to manage the policy templates on the SSLSM.
VLANs	Allows you to manage VLAN configurations on the SSLSM.
Statistics	Allows you to view the SSLSM statistics.

Selector

Figure 1-3 shows the selector; Table 1-4 describes the selector elements.

Figure 1-3 Selector

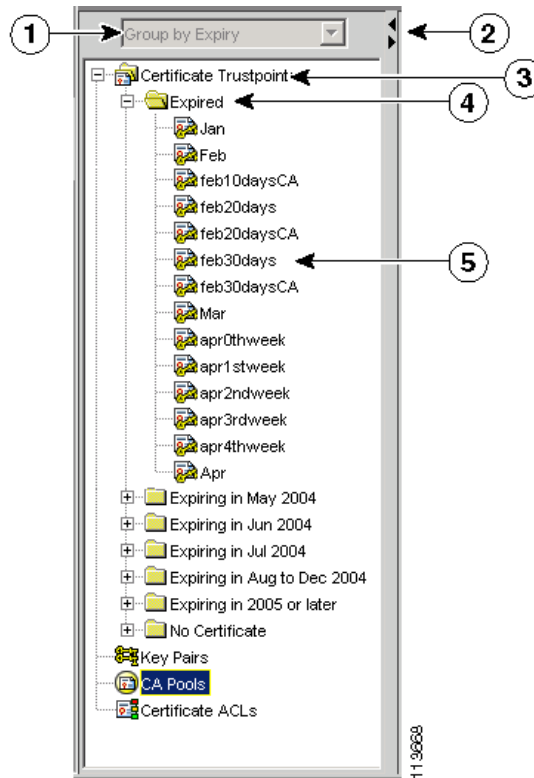


Table 1-4 Selector Elements

Figure 1-3 Reference	Location	Description
1	Object Grouper	You can group the objects using various parameters. Select your option from the list.
2	Selector handle	Click the handle to open and close the selector, or click the handle and drag it to resize it.
3	Group folder	Displays a group of objects. Click the plus (+) symbol to see the contents of this folder.
4	Subgroup folder	Displays a subgroup of objects. Click the plus (+) symbol to see the contents of this folder.
5	Object	Displays the individual entity contained in the group or subgroup. Click an object to open the page for that object.

**Note**

Figure 1-3 shows what the selector looks like when folders, subfolders, and objects are displayed. Not all selectors contain all of these elements.

Understanding the Action Buttons

This section describes the action buttons that appear in the CVDM-SSLISM dialog boxes and wizards.

- For a description of the wizard action buttons, see [Table 1-5 on page 1-20](#).
- For a description of the dialog box action buttons, see [Table 1-6 on page 1-20](#).

Table 1-5 *Wizard Action Buttons*

Button	Action
Back	Takes you to the previous page.
Next	Takes you to the next page.
Finish	Takes you to the wizard summary page.
Cancel	Exits the wizard without making any changes.
Help	Displays context-sensitive online help.

Table 1-6 *Dialog Box Action Buttons*

Button	Action
OK	Saves your changes.
Cancel	Exits the dialog box without making any changes.
Help	Displays context-sensitive online help.

Editing the Preferences

- Step 1** Select **Edit > Preferences...** The Preferences dialog box appears.
- Step 2** Modify the appropriate values:

GUI Element	Action/Description
Show CLI Preview for Wizards check box	<p>Select this checkbox if you want CVDM-SSLSM to display the CLI commands to be delivered to the device after you have completed a wizard.</p> <p>When this select this checkbox and click Finish in a wizard, the Deliver Configuration to the SSLSM dialog box opens and displays the CLI commands. For more information, see “Delivering CLI Commands to the Device” section on page 1-22.</p>
Show CLI Preview on Delivery check box	<p>Select this checkbox if you want CVDM-SSLSM to display the CLI commands to be delivered to the device.</p> <p>When this select the checkbox and click Deliver, the Deliver Configuration to SSLSM dialog box opens and displays the CLI commands. For more information, see “Delivering CLI Commands to the Device” section on page 1-22.</p>
Confirm before Exiting check box	<p>Select this checkbox if you want CVDM-SSLSM to confirm with you before exiting the application.</p> <p>Select the Always display this dialog box before exiting checkbox if you always want CVDM-SSLSM to confirm that you want to exit the application.</p>
Refresh after Delivery check box	<p>Select this check box to refresh CVM after delivering accumulated CLI commands for the device.</p>

Viewing Running Configuration

-
- Step 1** Select **View > Running Config > SSLSM...** The Running Configuration for SSLSM dialog box appears. Information about the running configuration for the SSL Services Module is displayed.
- Step 2** Click **Save to File...** to save the configuration information to a text file.
-

Delivering CLI Commands to the Device

You must deliver accumulated CLI commands to the device before any changes you make in CVDM-SSLSM will be applied.

-
- Step 1** Click the **Deliver** button at the top of the page. The Deliver Configuration to SSLSM dialog box appears if you have configured CVDM-SSLSM to display the accumulated CLI commands when you click the Deliver button.



Note The Deliver Configuration to SSLSM dialog box also appears when you click the **Finish** button in a wizard if you have configured CVDM-SSLSM to display the accumulated CLI commands after you have completed a wizard.



Note For Certificate Import and Export Wizards, Deliver CLI Commands dialog box will not appear.

- Step 2** Modify the appropriate values:

GUI Element	Action/Description
Save to Startup checkbox	Click the checkbox to save the running configuration, generated by CVDM, as the device startup configuration.
Deliver button	Click to send the accumulated CLI commands to the device.
Save to File... button	Click to save the CLI commands as a text file.
Close button ¹	Close the dialog box without delivering any CLI commands.
Deliver Later button ²	Click to deliver the wizard CLI commands to the device at a later time.

1. This button is available only in the Deliver Configuration to SSLSM dialog box that is displayed after you click **Deliver** at the top of the window.
2. This button is available only in the Deliver Configuration to SSLSM dialog box that is displayed after you click **Finish** in a wizard.

**Note**

For Certificate Wizards, Deliver Later option will be disabled. The task will be performed immediately at the end of the wizard.

**Note**

The Deliver Configuration to Switch/Module(s) dialog box displays *all* accumulated CLI commands that will be delivered to the device; therefore, any previous CLI commands that were not sent to the device are shown in this dialog box, as well as the CLI commands you have generated in this session.

What's Next?

You are about to set up an SSL Service. To set up the SSL service, first set up the Public Key Infrastructure. You need to configure Trustpoints and install the Key Pairs, Proxy Service Certificates, and the corresponding CA Certificates. You can use the Trustpoint wizards to setup the PKI.

Once the Proxy Service Certificates and Key Pairs are installed in the SSLSM PKI, the next task in setting up the SSL service is to configure Proxy Services. You can use the Proxy Service Wizard to setup up the SSL service to configure proxy service.



PART 2

SSL Services Module Management





PKI Overview

The following topics provide an overview of the public-key infrastructure (PKI):

- [Public Key Infrastructure, page 2-1](#)
- [Configuring Keys and Certificates, page 2-2](#)

Public Key Infrastructure

PKI is a system that manages encryption keys and identity information for the human and mechanical components of a network that participate in secured communications.

The SSL Services Module uses the SSL protocol to enable secure transactions of data through privacy, authentication, and data integrity; the protocol relies upon certificates, public keys, and private keys.

The certificates, which are issued by certification authorities and are similar to digital ID cards, verify the identity of the server to the clients and the clients to the server. The certificates include the name of the entity to which the certificate was issued, the entity's public key, and the time stamp that indicates the certificate's expiration date.

Public and private keys are the ciphers that are used to encrypt and decrypt information. The public key is shared without any restrictions, but the private key is never shared. Each public-private key pair works together; data that is encrypted with the public key can only be decrypted with the corresponding private key.

Configuring Keys and Certificates

You can configure keys and certificates using one of the following methods:

- If you are using Simple Certificate Enrollment Protocol (SCEP), configure the keys and certificates by doing the following:
 1. Generate a key pair.
 2. Declare the trustpoint.
 3. Get the certificate authority certificate.
 4. Send an enrollment request to a certificate authority on behalf of the SSL server.

See the [“Understanding Wizards” section on page 3-10](#) for details.

- If you are not using SCEP, configure the keys and certificates using the manual certificate enrollment (TFTP and cut-and-paste) feature by doing the following:
 1. Generate or import a key pair.
 2. Declare the trustpoint.
 3. Get the certificate authority certificate and enroll the trustpoint using TFTP or cut-and-paste to create a PKCS10 file.
 4. Request the SSL server certificate offline using the PKCS10 package.
 5. Import the SSL server certificate using TFTP or cut-and-paste.

See the [“Understanding Wizards” section on page 3-10](#) for details.

- If you are using an external PKI system, do the following:
 1. Generate PKCS12 or privacy enhanced mail (PEM) files.
 2. Import this file to the module.

See the [“Understanding Wizards” section on page 3-10](#) for details.

An external PKI system is a server or a PKI administration system that generates key pairs and enrolls for certificates from a certificate authority or a key and certificate archival system. The Public-Key Cryptography Standards (PKCS) specify the transfer syntax for personal identity information, including the private keys and certificates. This information is packaged into an encrypted file. To open the encrypted file, you must know a pass phrase. The encryption key is derived from the pass phrase.



Managing Certificates

A Trustpoint is an association of a CA Certificate, an RSA Key pair, and the corresponding SSL Client and Server Certificate.

The following topics are described in this section:

- [Getting started with Wizards, page 3-2](#)
- [Understanding Wizards, page 3-10](#)
- [Importing and Exporting Certificates, page 3-26](#)
- [Exporting Certificates in Bulk Using the Certificate Export Wizard, page 3-44](#)
- [Viewing Certificate Trustpoints, page 3-54](#)
- [Certificate Trustpoint Details, page 3-58](#)
- [Editing Trustpoint Configuration, page 3-68](#)
- [Deleting Certificates, page 3-74](#)
- [Certificate Hierarchy, page 3-73](#)
- [How Do I..., page 3-75](#)

Getting started with Wizards

The details below help you navigate as per the menu.

For more information on Wizards, see [Understanding Wizards, page 3-10](#)

Certificate Wizards

The certificate wizards help you to configure a certificate trustpoint using a wizard, Importing certificates and private keys, and export certificates and private keys.

Configuring a Certificate Trustpoint Using the Wizard

This wizard helps you to configure a certificate Trustpoint, generate the Certificate Signing Request (CSR), and install the SSL certificate obtained using the CSR.

The wizard also helps you to configure certificate authority (CA) Trustpoints and install a CA certificate or a CA certificate chain.

**Note**

If the CA issuing your certificate is a subordinate CA, then you must first install all of the CA certificates in the certification path.

Importing CA Certificate or CA certificate chain

-
- Step 1** Configure a trustpoint name. For details, see [Configuring a Trustpoint and RSA Key Pair, page 3-15](#)
- Step 2** Specify a CA certificate source. For details, see [Selecting a CA Certificate Source, page 3-19](#)
- Step 3** Specify a CA certificate. For details, see
- [Importing a CA Certificate Chain using Copy and Paste, page 3-22](#)
 - [Importing a CA Certificate Chain from a TFTP Server, page 3-23](#)
 - [Importing a CA Certificate Chain from a Local Hard Disk, page 3-21](#)
 - [Specifying a CA Certificate \(PEM\), page 3-37](#)

- Step 4** Select Trustpoint setup tasks. For details, see
- [Configuring Trustpoint Tasks, page 3-24](#)
 - [Viewing Wizard Summary, page 3-24](#)
 - [Delivering CLI Commands to the Device, page 1-22](#)
 - [Viewing Trustpoint Configuration Status, page 3-25](#)
-

Generating Certificate Signing Request (CSR)

- Step 1** Configure Trustpoints and RSA key pair. For details, see [Configuring a Trustpoint and RSA Key Pair, page 3-15](#)
- Step 2** Configure SSL certificate attributes. For details, see
- [Configuring SSL Certificate Attributes, page 3-16](#)
- Step 3** Configure enrollment parameters. For details, see
- [Configuring Enrollment Parameters, page 3-17](#)
- Step 4** Specify a CA certificate (for the copy-paste method only). For details, see
- [Specifying a CA Certificate \(PEM\), page 3-37](#)
- Step 5** Select Trustpoint setup tasks. For details, see
- [Configuring Trustpoint Tasks, page 3-24](#)
 - [Viewing Wizard Summary, page 3-24](#)
 - [Delivering CLI Commands to the Device, page 1-22](#)
 - [Viewing Certificate Signing Request \(CSR\), page 3-25](#)
-

Importing the SSL certificate

For more details, see [How do I import the SSL certificate obtained using CSR?, page 3-81](#).

Import Certificates and Private Key

This wizard lets you to import certificates and private key to SSLSM from an external public key infrastructure (PKI). You can import certificates in X.509 PEM, X.509 DER, PKCS#7, or PKCS#12 format. The instructions below guides you through the steps based on the format and source of the certificates.

Importing CA Certificate, SSL Certificate and Private Key.

To launch the task, see [Importing Certificates from an External PKI System, page 3-26](#)

Importing in PEM format- Local Hard Disk

- Step 1** Specify certificate formats and source. For details, see [Configuring Certificate Source and Format, page 3-28](#)
- Step 2** Specify certificates and private key files. For details, see
- [Configuring Certificates and Key Files \(PEM - Local Hard Disk\), page 3-35](#)
 - [Viewing the Summary, page 3-37](#)
 - [Viewing the Certificate Import Status, page 3-38](#)
-

Importing in PEM format- Copy-and-paste

- Step 1** Specify certificate formats and source. For details, see [Configuring Certificate Source and Format, page 3-28](#)
- Step 2** Specify CA certificate. For more details, see [Specifying a CA Certificate \(PEM\), page 3-37](#).
- Step 3** Specify Private Key [Specifying Private Key \(PEM Format\), page 3-37](#).
- Step 4** Specify SSL certificate. For more details, see:
- [Specifying SSL Certificate \(PEM Format\), page 3-37](#)

- [Viewing the Summary, page 3-37](#)
 - [Viewing the Certificate Import Status, page 3-38](#)
-

Importing in PEM format- Remote system

- Step 1** Specify certificate formats and source. For details, see
- [Configuring Certificate Source and Format, page 3-28](#)
- Step 2** Specify certificates and private key files.
- [Configuring Certificates and Key Files \(PEM - Remote System\), page 3-36](#)
 - [Viewing the Summary, page 3-37](#)
 - [Viewing the Certificate Import Status, page 3-38](#)
-

Importing in DER, PKCS#12, or PKCS#7

See the following sections:

- [Configuring Certificate Source and Format, page 3-28](#)
- [Viewing the Summary, page 3-37](#)
- [Viewing the Certificate Import Status, page 3-38](#)

Importing CA Certificate chain, SSL Certificate and Private Key

To launch the task, see [Importing Certificates from an External PKI System, page 3-26](#)

Importing in PEM - Local Hard Disk

- Step 1** Specify certificate format and source. For details, see [Configuring Certificate Source and Format, page 3-28](#)
- Step 2** Specify certificates and private key files. For details, see
- [Specifying Certificates and Private Key, page 3-32](#)

- [Viewing the Summary, page 3-37](#)
 - [Viewing the Certificate Import Status, page 3-38](#)
-

Importing in PEM- Copy- and- paste

- Step 1** Specify certificate format and source. For details, see [Configuring Certificate Source and Format, page 3-28](#)
- Step 2** Specify the CA certificates. For details, see [Specifying CA Certificates, page 3-34](#)
- Step 3** Specify private key. For details, see [Specifying Private Key \(PEM Format\), page 3-37](#)
- Step 4** Specify the SSL certificate. For details, see:
- [Specifying SSL Certificate \(PEM Format\), page 3-37](#)
 - [Viewing the Summary, page 3-37](#)
 - [Viewing the Certificate Import Status, page 3-38](#)
-

Importing in PKCS#12, or PKCS#7

See the following sections:

- [Configuring Certificate Source and Format, page 3-28](#)
- [Viewing the Summary, page 3-37](#)
- [Viewing the Certificate Import Status, page 3-38](#)

Export Certificates and Private Keys

This wizard lets you to export certificates and private keys from the SSLSM in PKCS#12 or PEM format. You can export certificates and private keys to an external system (local hard disk or remote server) or to another SSLSM. When exporting the certificates in PEM format, you can optionally choose to export the CA certificates in the certificate chain.

The instructions below guides you through the steps based on the format and source of the certificates.

To launch the task, do the following:

-
- Step 1** Click **Setup** in the CVDM-SSLSM task bar. The Setup page appears
 - Step 2** Click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.
 - Step 3** Select **Export Certificates and Private Keys**, then click **Launch the Selected Task**. The Certificate Export Wizard appears.
-

Exporting in PEM format- Local Hard Disk

-
- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
 - Step 2** Select a destination. For details, see [Specifying the Destination \(PEM\)](#), page 3-47.
 - Step 3** Specify the destination details. For details, see:
 - [Specify Destination Details \(PEM - Local Hard Disk\)](#), page 3-48
 - [Viewing Certificate Export Wizard Summary](#), page 3-43
 - [Viewing the Certificate Export Status](#), page 3-43
-

Exporting using Copy and Paste method

- Step 1** Select the certificates and format. For details, see
- [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45
- Step 2** Select a destination. For details, see
- [Specifying the Destination \(PEM\)](#), page 3-47
 - [Viewing Certificate Export Wizard Summary](#), page 3-43
 - [Viewing the Certificate Export Status](#), page 3-43
-

Exporting to Remote system

- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
- Step 2** Select a destination. For details, see [Specifying the Destination \(PEM\)](#), page 3-47.
- Step 3** Specify the destination details. For details, see
- [Specify Destination Details \(PEM - Remote System\)](#), page 3-49
 - [Viewing Certificate Export Wizard Summary](#), page 3-43
 - [Viewing the Certificate Export Status](#), page 3-43
-

Exporting to Redundant SSLSM

- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
- Step 2** Select a destination. For details, see [Specifying the Destination \(PEM\)](#), page 3-47.
- Step 3** Specify the destination details. For details, see
- [Specify Destination Details \(PEM - Redundant SSLSM\)](#), page 3-50

- [Viewing Certificate Export Wizard Summary](#), page 3-43
 - [Viewing the Certificate Export Status](#), page 3-43
-

PKCS#12

- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
- Step 2** Select a destination. For details, see [Specifying the Destination \(PKCS#12\)](#), page 3-51.
-

Exporting to Remote system

- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
- Step 2** Select a destination. For details, see [Specifying the Destination \(PKCS#12\)](#), page 3-51.
- Step 3** Specify the destination details. For details, see
- [Specify Destination Details \(PKCS#12 - Remote System\)](#), page 3-51
 - [Viewing Certificate Export Wizard Summary](#), page 3-43
 - [Viewing the Certificate Export Status](#), page 3-43
-

Exporting to Redundant SSLSM

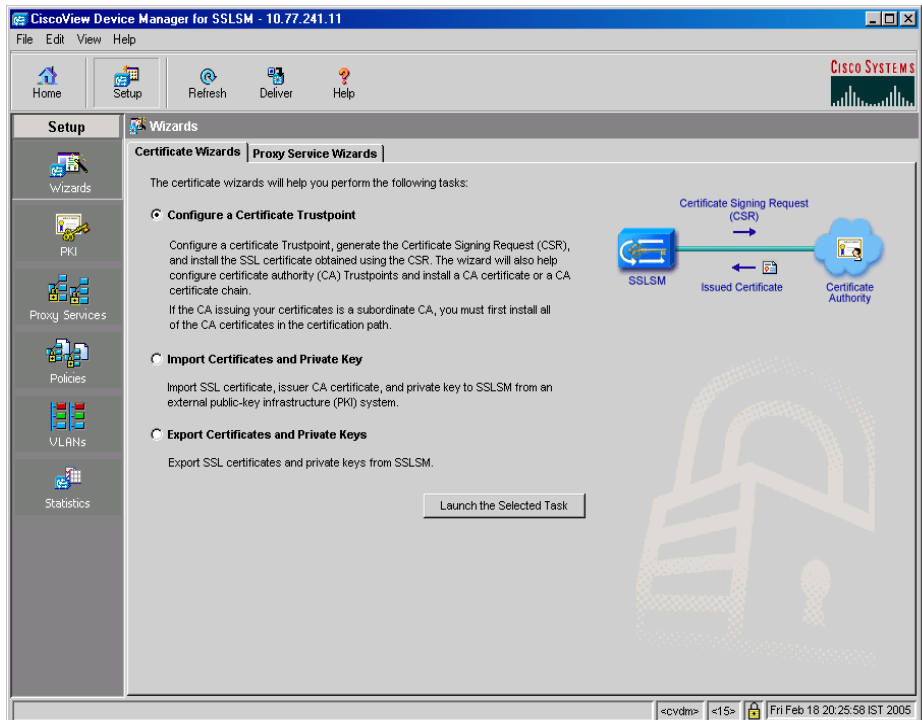
- Step 1** Select the certificates and format. For details, see [Selecting Certificates and Format \(PEM, PKCS#12\)](#), page 3-45.
- Step 2** Select a destination. For details, see [Specifying the Destination \(PKCS#12\)](#), page 3-51.
- Step 3** Specify the destination details. For details, see
- [Specify Destination Details \(PKCS#12 - Redundant SSLSM\)](#), page 3-52

- [Viewing Certificate Export Wizard Summary, page 3-43](#)
- [Viewing the Certificate Export Status, page 3-43](#)

Understanding Wizards

Wizards helps you to configure keys, certificates, and proxy services. You can access Certificate Wizards and Proxy Service Wizards from this page.

Figure 3-1 Wizards page



The following topics are included in this section:

Certificate Wizards

The Certificate Wizards helps you to configure keys and certificates. You can either create certificates and enroll them to the CA or import the certificates and the associated keys from an external PKI system. You can export the certificates and private keys using wizards.

- [Configuring a Certificate Trustpoint Using the Wizard, page 3-12](#)
- [Importing Certificates from an External PKI System, page 3-26](#)
- [Exporting Certificates Using the Wizard, page 3-38](#)
- [Exporting Certificates in Bulk Using the Certificate Export Wizard, page 3-44](#)

Proxy Service Wizards

The Certificate Wizards helps you to configure Proxy Services.

- [Basic Proxy Service Wizard, page 7-3](#)
- [Advanced Proxy Service Wizard, page 7-8](#)

Launching Certificate Wizards

To launch certificate wizards, do one of the following:

-
- Step 1** Click **Setup** in the task bar. The Setup page appears.
 - Step 2** Click **Wizard** in the left-most pane. The Wizards information page appears.
 - Step 3** Click the **Certificate Wizards** tab to create a CertificateTrustpoint.
You can select either of the following tasks:
 - Configure Certificate Trustpoint
 - Import Certificates and Private Key.
 - Export Certificates and Private Key.
 - Step 4** Select one of the tasks, then click **Launch the Selected Task**. The Trustpoint Setup wizard appears with information on the steps to follow.
-

Or:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**.
- Step 2** Click the **Setup Wizard** and select either of the following wizards:
- Configure Certificate Trustpoint
 - Import Certificates and Private Key.
 - Export Certificates and Private Key.
-

Configuring a Certificate Trustpoint Using the Wizard

You can use the wizard to configure a certificate Trustpoint, authenticate, and enroll with a CA using the wizard.

To configure a certificate trustpoint:

-
- Step 1** Click **Setup** in the task bar. The Setup page appears.
- Step 2** Click **Wizards** in the left-most pane. The Wizards information page appears.
- Step 3** Click the **Certificate Wizards**. The Certificate Wizards page appears.
- Step 4** Select **Configure Certificate Trustpoint**, then click **Launch the Selected Task**. The Trustpoint Configuration dialog box appears. The dialog box provides information on the steps to be followed to configure a Trustpoint.

You can use the wizard to configure either of the following Trustpoints:

- Proxy Service Trustpoint.
- CA Trustpoint.

Step 5 Click **Next** to continue.

Setting up a Proxy Service Trustpoint

You can use any one of the following options to set up a proxy service trustpoint:

- Create a new proxy service Trustpoint.
- Configure a proxy service Trustpoint using the copy-and-paste method.

To create a new Proxy Service Trustpoint:

- Step 1** Click **Setup** in the task bar. The Setup page appears.
- Step 2** Click **Wizard** in the left-most pane. The Wizards information page appears.
- Step 3** Click the **Proxy Service Wizards** tab to create a proxy service Trustpoint.
- Step 4** Configure Trustpoint name and RSA key pair.
- Step 5** (Optional) Configure SSL certificate attributes, then click **Next**.
- Step 6** Configure enrollment parameters, then click **Next**.
- Step 7** Select Trustpoint setup tasks, then click **Next**. The summary dialog box appears.
- Step 8** Click **Finish**. The Deliver Configuration to SSLSM dialog box appears with the details on the CLI commands to be delivered to the module.
- Step 9** Click **Deliver** to deliver the CLI commands. The Trustpoint Configuration Status dialog box appears.
-

To configure a Proxy Service Trustpoint using the copy-and-paste method:

-
- Step 1** Configure Trustpoint name and RSA key pair.
 - Step 2** (Optional) Configure SSL certificate attributes, then click **Next**.
 - Step 3** Configure enrollment parameters, then click **Next**.
 - Step 4** Specify CA certificate, then click **Next**.
 - Step 5** Select Trustpoint setup tasks, then click **Next**. Summary dialog box appears.
 - Step 6** Click **Finish**.
-

Setting up a CA Trustpoint

To configure a CA Trustpoint:

-
- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source.
-

To configure a CA Trustpoint using the copy-and-paste method:

-
- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source.
 - Step 3** Specify CA Certificate.
-

Configuring a Trustpoint and RSA Key Pair

The Configure Trustpoint and RSA Key Pair page helps you set up a proxy service Trustpoint or a CA Trustpoint. You can either use an existing key pair for the Trustpoint or generate a new key pair.



Note

If you are creating the Trustpoint for the first time, generate a new key pair. You will not be able to use an existing key pair.

The following fields appear:

Field	Action/Description
Trustpoint Name	You can add a new trustpoint or select an existing Trustpoint.
Trustpoint Type	
Proxy Service Trustpoint	Select this option to create a proxy service Trustpoint, generate CSR and, install the enrolled SSL certificate.
CA Trustpoint	Select this option to install a CA certificate or a CA certificate chain.
RSA Key Pair	
Generate a new Key Pair	Select this option to generate a new key pair.
Key Pair Name	Enter the name of the key pair. We recommend that you use a key pair name that matches the trustpoint name.
Key Size	The size of the key. Key size can be 512, 768, 1024, 1536, or 2048
Allow Private Key Export	Select this option to make the new key exportable. You need to select this to export the key at a later point of time.

Field	Action/Description
Use an Existing Key Pair	Select this option to use an existing key pair.
Key Pair Name	Select the key pair name.

Configuring SSL Certificate Attributes

The SSL Certificate Attributes wizard page allows you to enter the SSL certificate attributes for the certificate Trustpoint. Even though it is not mandatory to fill any of these fields, we recommend you to fill the common name (CN) field.

The following fields appear on the SSL certificate attributes dialog box:

Field	Description
Subject Distinguished Name (DN)	The fully qualified domain name in the certificate. The subject name uses Lightweight Directory Access Protocol (LDAP) format.
Common Name (CN)	The common name to be used. Example: server.domain.com, where server is the name of the SSL server that appears in the URL.
Email Address (EA)	E-mail address.
Organization Unit (OU)	Organization Unit. Example: Cisco
Department (D)	Name of the department. Example: Lab
Location (L)	The location of the organization. Example, San Jose
State (ST)	The name of the state. Example, California

Field	Description
Country (C)	The country name. Example: US
Include SSLSM Serial Number	Select this option to include the serial number of the SSLSM module in the certificate.
Unstructured	
Unstructured Name	The unstructured URL of the server. Example: server5.domain.com
Subject IP Address	IP address to be included in the certificate.
Other	
Certificate Purpose	Select between the options SSL Client and SSL Server.

Configuring Enrollment Parameters

The Configure Enrollment Parameters page of the wizard allows you to specify the enrollment parameters for your certificate authority.

The following field appears in the configure enrollment parameters page:

Field	Description
CA	The name of the certificate authority. <ul style="list-style-type: none"> If you are configuring enrollment parameters for a new CA, choose the field display as <NEW>. If you want to enroll with a CA already configured, select the CA from the list and modify the parameters.
Simple Certificate Enrollment Protocol (SCEP)	Select this to use the SCEP.

Field	Description
CA Server URL	URL of the CA server.
Challenge Password	Enter a Challenge Password .
Confirm the Password	Confirm the challenge password.
Retry Count	Number of retries.
Enable Auto-Enrollment	Select to enable auto-enrollment.
Retry Period (Minutes)	Time to wait for the next retry.
HTTP Proxy	URL of the HTTP proxy to be used for the enrollment.
Port	The port to be used for the enrollment.
TFTP	Select this if you are using TFTP.
CA Server URL	URL of the CA server. Example: tftp://ipaddress/Certificates/filename The suffix <i>.ca</i> is appended to the file name.
Copy and Paste / Local Hard Disk	Select this option to Copy-and-Paste the Certificate or specify Certificate from the local Hard Disk.

The TFTP and cut-and-paste feature allows you to generate a certificate request and accept certification authority certificates as well as router certificates. These tasks are accomplished with a TFTP server or manual cut-and-paste operations.

You may want to use TFTP or manual cut-and-paste enrollment in the following situations:

- Your certificate authority does not support Simple Certificate Enrollment Protocol (SCEP).
- A network connection between the router and certificate authority is not possible. The router running Cisco IOS software obtains its certificates using a network connection between the router and the certificate authority.

Selecting a CA Certificate Source

The CA Certificate Source page of the wizard allows you to specify the source of the CA certificate. You can import a CA certificate or a CA certificate chain. You can import a certificate chain using X.509 PEM or PKCS#7 format. You can select any of the following formats:

- X.509 PEM
- X.509 DER
- PKCS#7



Note

To import the certificate using SCEP, select the PKCS#7 format.

If you have selected X.509PEM, the following options appear:

- **Local Hard Disk**—Select this option to import the CA certificate from the client machine.
- **Copy and Paste**—Select this option to import the CA certificate using copy and paste method.
- **TFTP**—Select this option to import the CA certificate from a TFTP server.
- Select the **Import a CA Certificate Chain** check box to import the certificate chain.

If you have selected X.509 DER, you need to select the CA Certificate File. Click Browse and browse to the directory where you have the certificate file, then select the file.

If you have selected PKCS#7, the following fields appear:

Field	Description
Simple Certificate Enrollment Protocol (SCEP)	Select this option to import file using SCEP.
CA Server URL	Enter the URL of the CA Server.
Local Hard Disk	Select this option to import a file from the local hard disk.

Field	Description
PKCS#7 File	Click Browse and browse to the directory where you have the PKCS#7 file, then select the file.
PKCS#7 CA Certificates	
CRL Verification	Options are: <ul style="list-style-type: none"> • Strict (Default) • Optional • Best Effort
CA Level	Level of CA in the certificate chain.
CA Name	Name of the CA.
Trustpoint Name	Name of the Trustpoint to which the CA certificate is imported.

Click **Next** to continue.

Importing a CA Certificate Chain

You can specify all the certificates in a certificate chain and the wizard will create CA Trustpoints for each of the CA certificate.

A suffix is added to Trustpoint name based on whether the CA certificate is a root or sub-ordinate CA certificate. You can edit the default Trustpoint name by using the CA Trustpoints tab. As the certificates are added, the status of the certificate and certificate chain is displayed.

To import a CA certificate chain:

-
- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source as X.509 PEM.
 - Step 3** Select the source from where you want to import the certificate chain. The options are: **Local Hard Disk**, **Copy and Paste**, **TFTP**.
 - Step 4** Select **Import a CA Certificate Chain** check box.

- If you have selected Local Hard Disk, see [Importing a CA Certificate Chain from a Local Hard Disk, page 3-21](#).
 - If you have selected Copy and Paste, see [Importing a CA Certificate Chain using Copy and Paste, page 3-22](#).
 - If you have selected Local Hard Disk, see [Importing a CA Certificate Chain from a TFTP Server, page 3-23](#).
-

Importing a CA Certificate Chain from a Local Hard Disk

- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source as X.509 PEM.
 - Step 3** Select **Local Hard Disk**.
 - Step 4** Select **Import a CA Certificate Chain** check box, then click **Next**. The Specify CA Certificate page appears.
 - Step 5** Specify the CA certificates in the **CA Certificate Chain**
 - Step 6** Click **Next** to continue.
-

To specify the certificates in the certificate chain:

- Step 1** Click **Add**. The Add a Certificate popup window appears.
- Step 2** Click **Browse** to browse to the directory where you have the certificate file and select it.
- Step 3** Click **OK**.

**Note**

When specifying the certificates in the certificate chain, add Root CA through the subordinate CA in accordance with the certificate hierarchy.

Importing a CA Certificate Chain using Copy and Paste

- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source as X.509 PEM.
 - Step 3** Select **Copy and Paste**.
 - Step 4** Select **Import a CA Certificate Chain** check box, then click **Next**. The Specify CA Certificate page appears.
 - Step 5** Specify the CA certificates in the **CA Certificate Chain**.
 - Step 6** Click **Next** to continue.
-

To specify the certificates in the certificate chain:

- Step 1** Click **Add**. The Add a Certificate popup window appears.
- Step 2** Copy and Paste the certificate in PEM format to the Certificate field.
Click **Clear** to remove the content or click **View Details** to view the details of the certificate.
- Step 3** Click **OK** to add the certificate.



Note When specifying the certificates in the certificate chain, add Root CA through the subordinate CA in accordance with the certificate hierarchy.

Importing a CA Certificate Chain from a TFTP Server

To import a CA certificate chain from a TFTP server:

-
- Step 1** Configure Trustpoint Name.
 - Step 2** Specify CA Certificate source as **X.509 PEM**.
 - Step 3** Select **TFTP**.
 - Step 4** Select **Import a CA Certificate Chain** check box, then click **Next**. The Specify CA Certificate page appears.

Specify the CA certificate in the certificate chain. You must specify all certificates in the chain from root CA.

The following fields appear:

Field	Description
CA Level	Level of CA in the certificate chain.
CA Certificate File	URL (TFTP) of the CA certificate.
Trustpoint Name	Name of the Trustpoint to which the CA certificate is imported.

You can add certificates to the list. To add a CA certificate:

-
- Step 1** Click **Add**. The Add a Certificate popup window appears.
 - Step 2** Enter the TFTP Server IP address.
 - Step 3** Enter the file name. The certificate file name must have a.ca extension.



Note The validity of the certificate or the completeness of the certificate chain is not validated. Please make sure that you specify valid CA certificates and all the certificates are in the certificate chain.

**Note**

When specifying the certificates in the certificate chain, add Root CA through the subordinate CA in accordance with the certificate hierarchy.

Configuring Trustpoint Tasks

The Trustpoint Setup Tasks wizard page allows you to select a Trustpoint configuration task that you want to perform on the certificate Trustpoint.

You can select one of the following tasks:

Field	Action/Description
Generate CS R (Enroll)	Select this option to apply the trustpoint configuration, authenticate the CA certificate, and generate certificate request (enroll).
Authenticate the CA Certificate	Select this option to apply the trustpoint configuration and authenticate the CA certificate
Import SSL Server Certificate	Select this option to apply the Trustpoint configuration and import the SSL certificate. This is applicable only to manual enrollment methods.

Viewing Wizard Summary

When you use a wizard to perform a configuration, the wizard's Summary page displays the values that you have configured. You can examine those values and click the wizard's Back button to return to a screen on which you need to make a change. When you have made the changes, click the Finish button to save your changes and leave the wizard.

Delivering Configuration to an SSL Module

This page provides information on the CLI commands you have configured.

Click **Deliver** to deliver the commands to the module

Click **Save to File** to save the commands to a file.

Click **Deliver Later** to deliver the commands at a later point of time.

For more information on delivering CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#)

Viewing Trustpoint Configuration Status

The Trustpoint Configuration Status dialog box provides the status details of the Trustpoint configuration tasks. The details displayed vary according to the task you selected. The dialog box displays the status against each task. The configuration performed on the module is displayed in the content area. If any task fails, you can review the task details and take necessary action.

Click **OK** to view the Certificate Signing Request (CSR). For more information on Certificate Signing Request (CSR), see [Viewing Certificate Signing Request \(CSR\), page 3-25](#)

For authentication, after displaying the status, the finger print information appears. Verify the finger print displayed and accept the certificate to complete the authentication.

Viewing Certificate Signing Request (CSR)

The Certificate Request dialog box provides information on the certificate requested.

Click **Save to File** to save the certificate request. The file is saved with the default extension.*csr*.

Click **Cancel** to close the dialog box.

Importing and Exporting Certificates

You can use wizards to import and export certificates. This section contains the following information:

- [Importing Certificates from an External PKI System, page 3-26](#)
- [Exporting Certificates Using the Wizard, page 3-38](#)
- [Exporting Certificates in Bulk Using the Certificate Export Wizard, page 3-44](#)

Importing Certificates from an External PKI System

The Certificate Wizard allows you to import Certificates and Private Keys from an external PKI. You can import certificates in X.509 PEM, X.509 DER, PKCS#7, or PKCS#12 format.

To import certificates using Trustpoint Wizard:

-
- Step 1** Click **Setup** in the CVDM-SSLSM task bar. The Setup page appears
 - Step 2** Click **Wizards** in the left-most pane. The dialog box appears.
 - Step 3** Select **Import Certificates and Private Key**, then click **Launch the Selected Task**. The Certificate Import Wizard appears.

You can import files in either of the following formats:

- X.509 PEM file, See [Importing PEM File, page 3-27](#).
 - PKCS#12 file, See [Importing PKCS#12 File, page 3-26](#).
 - X509 DER file
 - PKCS#7 file
-

Importing PKCS#12 File

You can use an external PKI system to generate a PKCS#12 file and then import this file to the module.

When creating a PKCS#12 file, include the entire certificate chain, from server certificate to root certificate, and public and private keys. You can also generate a PKCS#12 file from the module and export it.

**Note**

Imported key pairs cannot be exported.

If you are using SSH, we recommend using SCP when importing or exporting a PKCS#12 file. SCP authenticates the host and encrypts the transfer session.

To import a PKCS#12 File:

-
- Step 1** Enter certificate format and source, then click Next. The Summary dialog box appears.
 - Step 2** Click **Finish** to complete importing the certificate.
-

Importing PEM File

To import a PEM File:

-
- Step 1** Enter the format and source.
 - Step 2** Specify the certificate and key Files.
 - Step 3** Specify the private key.
 - Step 4** Specify SSL certificate.
 - Step 5** Click **Next**. The summary dialog box appears.
 - Step 6** Click **Finish** to complete importing the file.
-

You can copy and paste the CA Certificate in PEM format.

To import a PEM File using the copy-and-paste method:

-
- Step 1** Enter the format and source

- Step 2** Copy-and-paste the CA Certificate in PEM format.
- Step 3** Click **Next**. The summary dialog box appears.
- Step 4** Click **Finish** to complete importing the file.
-

Configuring Certificate Source and Format

The Certificate Source and Format page of the wizard allows you to enter the Trustpoint name, format and source.

You can select any of the following formats and select the source of the certificates and private key:

- X.509 PEM
- PKCS#12
- X.509 DER
- PKCS#7

X.509 PEM

- Step 1** Select one of the following PEM formats:
- Local Hard Disk—to import certificates from the client workstation.
 - Copy and Paste—to import certificates and key using copy-and-paste method.
 - Remote system—to import certificates from a remote system using TFTP, FTP, RCP, or SCP.
- Step 2** (Optional) Select **Import Certificate Chain** to import the certificate chain associated with the Trustpoint. (This option is available only if you select Local Hard Disk or Copy and Paste)
- Step 3** Select one of the option, then click **Next**.

- If you have selected Local Hard Disk and Import Certificate Chain, the next step is specifying certificates and key pairs.
- If you have selected Copy and Paste, and Import Certificate Chain, the next step is specifying CA certificates.

PKCS#12

Step 1 Select PKCS#12, the following fields will be displayed:

Field	Description
Protocol	Select any of the following protocols to be used for importing the file: <ul style="list-style-type: none"> • TFTP • FTP • RCP • SCP
IP Address	IP address of the certificate source.
User Name	User name for the remote system.
Password	Password to be used for the remote system.
PKCS#12 File	File name with the absolute path and the file name. Example: d:/tftpboot/certs/cert.p12
Passphrase	Passphrase to be used to decrypt the key.
Create Trustpoints for CA Certificates in Certificate Chain	Select this is to create Trustpoints for certificates higher in the hierarchy.

X.509 DER

Field	Description
CA Certificate File	Click Browse and select the certificate file from the directory.
Private Key File	Click Browse and select the certificate file from the directory.
Private Key Passphrase	Enter the Passphrase for the private key.
NET Format (Netscape Server/Microsoft IIS)	For private key in NET format, you must specify the RC4 passphrase used to encrypt the key. The same passphrase will be used to encrypt the private key in PEM format.
SGC Key	This is active only for NET Format key.
Allow Private Key Export	Select the check box to allow exporting the private keys.

PKCS#7

The wizard will use the following suffixes when creating the CA Trustpoints:

- Root CA Certificate: -rootCA
- Sub-ordinate CA Certificate: -subCA<level>

Field	Description
PKCS#7 Certificate File	Click Browse and select the certificate file from the directory.
Create Trustpoints for CA Certificates in Certificate Chain	Select this option to create Trustpoints for certificates in a chain. On selecting this check box a new set of field details appears below. For details see PKCS#7 CA Certificates field in the same table.

Field	Description
Private Key File (PEM)	Click Browse and select the certificate file from the directory.
Private Key Passphrase	Passphrase to be used to decrypt the key.
Allow Private Key Export	Select the check box to allow exporting the private keys.
PKCS#7 CA Certificates	This field appears only if you select Create Trustpoints for CA certificates in Certificate Chain option. It provides the list of CA certificates in the PKCS#7 file.
CRL Verification	You can select any option given below: <ul style="list-style-type: none"> • Strict (default) • Optional • Best Effort This selected option applies to the entire table below.
The table below provides the list of CA certificates in the PKCS#7 file.	
CA Level	The level of the CA in the certificate chain.
CA Name	The name of the certification authority.
Trustpoint Name	The name of the trustpoint associated with the certificate.

A passphrase protects a PEM file that contains a private key. The PEM file is encrypted by DES or 3DES.

Enter the details, then click **Next**.

Specifying Certificates and Private Key

If you have selected to import a certificate chain in X.509 PEM format from the local hard disk you need to specify the CA certificates, SSL (Server/Client) certificate and private key.

You must specify all CA certificates in the chain from the root CA to the issuer of the SSL certificate.

The following fields appear:

Fields	Description
CA Certificate Chain	
CRL Verification	<p>Select the level of verification. It can be one of the following:</p> <ul style="list-style-type: none"> • Strict • Optional • Best Effort
Chain	<p>Add the certificate in the chain.</p> <p>Add—Click Add to add a CA certificate to the chain. A popup dialog box appears.</p> <p>Enter the CA Trustpoint Name, The certificate in PEM format is displayed.</p> <p>Click View Details to view the details of the CA Certificate.</p> <p>Click OK to complete adding the certificate.</p> <p>Remove—Select a certificate from the chain, then click Remove to remove the CA certificate from the chain.</p>

Fields	Description
CA Trustpoints	<p>Provides the details of the CA Trustpoints.</p> <p>You can specify the name of the Trustpoint and can even edit the name of the Trustpoint.</p> <p>CA Level—Level of the CA in the certificate chain.</p> <p>CA Name—The name of the certification authority.</p> <p>Trustpoint Name—Name of the trustpoint associated with the certificate.</p> <p>Select a CA Trustpoint, then click Edit to edit the CA Trustpoint.</p>
SSL Certificate and Private Key File	
SSL Certificate File	Click Browse , and navigate to the folder where you have the SSL Certificate file.
Private Key File	Click Browse , and navigate to the folder where you have the Private Key file.
Private Key Passphrase	Passphrase to be used to decrypt the private key.
Allow Private Key Export	Select this check box if you want to allow the private key to be exported.

Specifying CA Certificates

If you have selected to import a certificate chain in X.509 PEM format using the copy and paste method, you need to specify the CA certificates from the root CA to the issuer of the SSL certificate. The following fields appear:

Field	Description
CA Certificate Chain	
CRL Verification	<p>Select the level of verification. It can be one of the following:</p> <ul style="list-style-type: none"> • Strict • Optional • Best Effort
Chain	<p>Displays the certificate chain.</p> <p>Add—Click Add to add a CA certificate to the chain. A popup dialog box appears.</p> <p>Enter the CA Trustpoint Name, The certificate in PEM format is displayed.</p> <p>Click View Details to view the details of the CA Certificate.</p> <p>Click OK to complete adding the certificate.</p> <p>Remove—Select a certificate from the chain, then click Remove to remove the CA certificate from the chain.</p>
CA Trustpoints	<p>Provides the details of the CA Trustpoints.</p> <p>CA Level—Level of the CA in the certificate chain.</p> <p>CA Name—The name of the certification authority.</p> <p>Trustpoint Name—Name of the trustpoint associated with the certificate.</p> <p>Select a CA Trustpoint, then click Edit to edit the CA Trustpoint.</p>

Click **Next** to continue.

Configuring Certificates and Key Files (PEM - Local Hard Disk)

The Certificates and Key Files dialog box allows you to specify the location of the certificates and key files.

The following fields are displayed:

Field	Description
CA (Certificates Issuer)	To create a new CA, specify the CA (issuer of the SSL certificate) certificate, private key and SSL certificate files you want to import. If the CA certificate is available on the SSLSM select the corresponding CA name.
CA Certificate File	The CA certificate file name with the absolute path. You can browse and select the file from the local hard disk.
Private Key File	The private key file name with the absolute path. You can browse and select the file from the local hard disk.
Private Key Passphrase	The passphrase to decrypt the key.
Allow Private Key	Select the check box to allow the private key export facility.
SSL Certificate File	The SSL certificate file name with the absolute path. You can browse and select the file from the local hard disk.



Note

A passphrase protects a PEM file that contains a private key. The PEM file is encrypted by DES or 3DES. The encryption key is derived from the pass phrase. A PEM file containing a certificate is not encrypted and is not protected by the pass phrase.

Configuring Certificates and Key Files (PEM - Remote System)

The Certificates and Key Files dialog box allows you to specify the location of the certificates and key files.

The following fields appear:

Field	Description
Protocol	Select the protocol to be used for importing the file. You can select any of the following protocols: <ul style="list-style-type: none"> • TFTP • FTP • RCP • SCP
IP Address	IP address of the remote system.
Username	User name for the remote system.
Password	Password for the remote system.
CA Certificate File	The CA certificate file name with the absolute path. Enter the absolute path and the file name. Example: /Certs/cert.pem
Private Key File	The Private Key file name with the absolute path. Enter the absolute path and the file name. Example: /Certs/cert.pem
Passphrase	The passphrase to decrypt the key.
SSL Certificate File	The SSL certificate file name with the absolute path. Example: /user/local/Certs/cert.pem

**Note**

A passphrase protects a PEM file that contains a private key. The PEM file is encrypted by DES or 3DES. The encryption key is derived from the pass phrase. A PEM file containing a certificate is not encrypted and is not protected by the pass phrase.

Specifying a CA Certificate (PEM)

This page of the wizard allows you to copy-and-paste the CA certificate in PEM format.

In Certificate Trustpoint Setup Wizard you can browse and specify the CA certificate file.

In Certificate Import Wizard you can select the CA certificate from the CA (Certificate Issuer) drop-down list. If you select any of the CA, the certificate details are displayed.

Click **Next** to continue.

Specifying Private Key (PEM Format)

Copy and paste the RSA private key in PEM format and enter the passphrase used to protect the key.

Click **Next** to continue.

Specifying SSL Certificate (PEM Format)

Copy and paste the SSL Certificate in PEM format.

Click **Next** to continue.

Viewing the Summary

When you use a wizard to perform a configuration, the wizard's Summary screen displays the summary of the certificate you are about to import.

You can examine the values and click the Back button to return to a screen on which you need to make a change. When you have made the changes, click the Finish button to import the certificate and leave the wizard.

Delivering Configuration to SSL Module

This page provides information on the CLI commands you have configured.

Click **Deliver** to deliver the commands to the module

Click **Save to File** to save the commands to a file.

Click **Deliver Later** to deliver the commands at a later point of time.

For more information on delivering CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#)

Viewing the Certificate Import Status

The certificate import status dialog box provides the status details of the Trustpoint configuration tasks. The details displayed vary according to the task you selected. The dialog box displays the status against each task.

The configuration performed on the module is displayed in the content area. If any task fails, you can review the task details and take necessary action.

Exporting Certificates Using the Wizard

You can export certificates using either PKCS#12 file format or privacy-enhanced mail (PEM) file format.

Exporting certificates of more than one Trustpoint

To export certificates of more than one Trustpoint, see [Export Certificates and Private Keys, page 3-7](#).

Exporting certificates of a selected Trustpoint

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select Trustpoints from the object [Selector](#). The Trustpoint page appears.
 - Step 2** Select a Trustpoint node from the logical group. You can group the Trustpoints using Trustpoint Grouper.
 - Step 3** Select a **Trustpoint** from the list.

- Step 4** Click **Operations**, then select **Export** from the popup menu.
- Step 5** The Trustpoint Export Wizard appears.
- You can export Trustpoints in using PKCS#12 or PEM format.
-

For more information on exporting Trustpoints in PKCS#12 file format, see [Exporting PEM Files, page 3-40](#).

For more information on exporting Trustpoints in PKCS#12 file format, see [Exporting PKCS#12 Files, page 3-39](#).

Exporting PKCS#12 Files

To export a PKCS#12 File:

- Step 1** Enter **Certificate Format and Destination**, then click **Next**. The summary page appears.
- Step 2** Click **Finish** to complete exporting the file.
-

Exporting PEM Files

To export a PEM File:

-
- Step 1** Enter certificate format and destination, then click **Next**.
You can select any of the following:
- Local Hard Disk—to export certificates and keys to the client workstation.
 - Copy-and-Paste—to export certificates and keys using copy-and-paste method.
 - Remote System—to export certificates and keys using TFTP, FTP, RCP or SCP.
- Step 2** Specify Certificate and Key files. The fields change depending on the source you have selected.
- Step 3** Click **Finish** to complete exporting the files.
-

Certificate Format and Destination

The Certificate Format and Destination page of the wizard allows you to specify the Trustpoint name and then select the format and destination.

The dialog box displays following fields:

Field	Description
Trustpoint Name	The name of the Trustpoint.
Pass phrase	The pass phrase to be used for decrypting the key.
Encryption	The encryption to be used for the key pairs.
Format	The file format. Options are PEM and PKCS#12.

If you select PEM, the following fields appear:

Field	Description
Local Hard Disk	Select to export certificates and keys to the client workstation
Copy and Paste	Select to export certificates and keys through copy-and-paste.
Remote System	Select to export certificates and keys using TFTP, FTP, RCP or SCP.

If you select PKCS#12, the following fields appear:

Field	Description
Protocol	The protocol used for the transferring the keys.
IP Address	The IP address of the destination system.
User Name	The user name for the destination system.
Password	The password to be used for the destination system.
PKCS#12 Certificate File	Specify the PKCS#12 file format.

Certificate and Key Pair Files (PEM - Local Hard Disk)

The Certificate and Key Pair Files (PEM Local Hard Disk) page of the wizard allows you to export PEM files from your local hard disk.

The following fields appear:

Field	Description
CA Certificate File	Enter the CA Certificate file name with the absolute path. Alternatively, you can browse and select the file from the local hard disk.
Private Key File	Enter the Private Key File name with the absolute path. Alternatively you can browse and select the file from the local hard disk.
SSL Certificate File	Enter the SSL Certificate File name with the absolute path. Alternatively you can browse and select the file from the local hard disk.

Certificate and Key Pair Files (PEM - Remote File System)

The Certificate and Key Pair File (PEM Remote File System) page of the wizard allows you to export a PEM file from a remote file system.

This page allows you to protocol, certificate and private key file destination details.

The following fields appear:

Field	Description
Protocol	Protocol to be used for exporting the file.
IP Address	IP address of the remote system.
User Name	User name for the remote system.
Password	Password for the remote system.

Field	Description
CA Certificate File	The absolute path to the CA Certificate file. Example:/certs/cert.pem
Private Key File	The absolute path to the Private Key file. Example:/certs/cert.pem
SSL Certificate File	The absolute path to the SSL Certificate file. Example:/certs/cert.pem

Viewing Certificate Export Wizard Summary

When you use a wizard to perform a configuration, the wizard's Summary page displays the values that you have configured. You can examine those values and click the wizard's Back button to return to a screen on which you need to make a change. When you have made the changes, click the **Finish** button to save your changes and leave the wizard.

Viewing the Certificate Export Status

The certificate export status dialog box provides the status details of the certificate export tasks. If the task fails, you can review the task details and take necessary action.

Exporting Certificates in Bulk Using the Certificate Export Wizard

The Certificate Export Wizard allows you to select multiple Certificates and Private Keys and export them.

To export certificates using Certificate Export Wizard:

-
- Step 1** Click **Setup** in the CVDM-SSLSM task bar. The Setup page appears
 - Step 2** Click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.
 - Step 3** Select **Export Certificates and Private Keys**, then click **Launch the Selected Task**. The Certificate Export Wizard appears.

You can export the certificates in either of the following formats:

- X.509 PEM
- PKCS#12

To export certificates and private keys in X.509 PEM format:

-
- Step 1** Select Certificates and Format (X.509).
 - Step 2** Specify the Destination Details
 - Step 3** View the Status.

To export certificates and private keys in PKCS#12 format:

-
- Step 1** Select Certificates and Format (X.509).
 - Step 2** Select the Destination.
 - Step 3** Specify the Destination details.
-

Selecting Certificates and Format (PEM, PKCS#12)

This page of the wizard helps you to specify the certificates to be exported and the format in which you want them to be exported.

The certificates are listed in the Certificates table. The following fields are displayed:

Field	Description
SSL Certificate Subject	The subject of the SSL certificate.
Certificate TrustPoint	The Trustpoint name of the certificate.

Select **Export CA Certificate in the Chain** to export the CA Certificates in the certificate chain of the selected certificates.

You can add and remove Certificates from the list:

- Click **Add** to add certificates to the export list. A popup window appears with the list of Trustpoints and Proxy Services. Select the Trustpoint or proxy services from the list, then click **OK**.
- Select a certificate and click **Remove** to remove a certificate from the export list.

Select the Format in which you want to export the certificate. You can export the certificates in X.509 PEM format or PKCS#12 format.

If you have selected X.509 PEM format, specify the following:

Field	Description
Encryption	The following are the encryption options: 3DES
Passphrase	Enter the passphrase.
Confirm Passphrase	Re-enter the passphrase to confirm.

Select the check box against **Export CA Certificates in certificate chains** to enable the export of the CA certificates in certificate chains.

If you have selected PKCS#12, specify the following:

Field	Description
Passphrase	Enter the passphrase.
Confirm Passphrase	Re-enter the passphrase to confirm.

Adding Certificates and Trustpoints for exporting

To add certificates and trustpoints to the export list:

- Step 1** Click **Setup** in the CVDM-SSLSM task bar. The Setup page appears.
- Step 2** Click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.
- Step 3** Select **Export Certificates and Private Keys**, then click **Launch the Selected Task**. The Certificate Export Wizard appears.
- Step 4** Click **Add**. A popup window appears with the list of Trustpoints and Proxy Services.
- Step 5** Click the tabs to select **Trustpoint** or **Proxy Services**.
- Step 6** Select the Trustpoint or Proxy Service from the list.
- Step 7** If you select Trustpoint, the following fields appear:

Field	Description
Trustpoint Name	The name of the Trustpoint.
Subject Name	The name of the subject.
Issuer Name (CA)	The name of the issuer.

- Step 8** Select a Trustpoint Name and click **OK** to add or click **Cancel** to close the window.
- Step 9** If you select Proxy Services, the following fields appear:

Field	Description
Proxy Service Name	The name of the proxy service.
Subject Name	The name of the subject.
Issuer name (CA)	The name of the issuer.

Step 10 Select a Proxy Service Name and click **OK** to add or click **Cancel** to close the window.

Specifying the Destination (PEM)

You can select any one of the following destination for the X.509 Format:

- Local Hard Disk—To export the certificate and private key to this client machine.
- Copy and Paste—To export the certificates and private key using copy and paste method.
- Remote System—To export the certificates and private keys to a remote server using TFTP, FTP, SCP, or RCP.
- Redundant SSLSM—To export the certificates and private keys to a redundant SSL services module.



Note

Copy and Paste and Remote System options will be disabled if you select more than one certificate.

Specify Destination Details (PEM - Local Hard Disk)

You can specify the destination details using this page.

The following fields are displayed:

Fields	Description
Directory	Click the Browse button and browse to the directory where you want the certificate to be exported.
Trustpoint	Displays the name of the trustpoint.
CA Certificate File	Displays the CA certificate chain names.
SSL Certificate File	Displays the SSL certificate chain names.
Private Key File	Displays the Private Key option file names.

If you have selected the **Export CA Certificate in Certificate Chains** in the step 1 then the CA Certificates in Certificate Chains table with the following details are displayed.

Fields	Description
Certificate Authority (CA) Name	Displays the chain of certificate authority names.
CA Certificate File	Displays the chain of CA certificate file names.

Click **Next** to continue.

Specify Destination Details (Copy and Paste)

This page is enabled only when exporting a single Trustpoint. Once the export is completed, exported certificates and private keys are displayed. You can copy and paste the certificate and save the file.

Specify Destination Details (PEM - Remote System)

Specify the details of the Remote system where you want the certificates and private keys to be exported.

The following fields are displayed:

Fields	Description
File Server	
Protocol	Select from options: <ul style="list-style-type: none"> • FTP • RCP • SCP • TFTP
Server IP Address	Enter the IP address of the system.
Username	Enter the user name
Password	Enter the password.
Files	
Directory	Enter the path or location of the files.
Trustpoint	Displays the name of the Trustpoint.
CA Certificate File	Displays the name of the CA Certificate files.
SSL Certificate File	Displays the name of the SSL Certificate files.
Private Key File	Displays the name of the Private key files.

To edit the CA certificate, SSL certificate, and, Private Key, select the Trustpoint name in the table and click **Edit**.

Click **Next** to continue.

Specify Destination Details (PEM - Redundant SSLSM)

You can export certificates to a redundant SSLSM. The Wizards will use the same Trustpoint name as the selected Trustpoint on the redundant SSLSM. You can edit the names if required.



Note

Do not specify a Trustpoint name that already exists in the redundant SSLSM. If the Trustpoint name is already present, the export will fail.

The following fields are displayed:

Field	Description
Redundant SSLSM	
IP Address	Enter the IP address of the redundant SSLSM.
User Name	Enter the user name.
Password	Enter password.
Enable Username	Re-enter the user name to enable the user
Enable Password	Re-enter the password to confirm.
Trustpoints	
SSL Certificate Subject	Displays the list of SSL certificates.
Redundant SSLSM Trustpoint	Displays the list of redundant trustpoints of SSLSM

To edit the redundant SSLSM Trustpoint Name select the row in the table and click **Edit**.

If you have selected the **Export CA Certificate in Certificate Chains** in the step 1 then the CA Certificates in Certificate Chains table with the following details are displayed.

Fields	Description
Certificate Authority (CA) Name	Displays the chain of certificate authority names.
Redundant SSLSM Trustpoint	Displays the list of redundant trustpoints of SSLSM
CRL Verification	Select the CRL verification from the given options.

To edit the redundant SSLSM Trustpoint Name select the row in the table and click **Edit**.

Click **Next** to continue.

Specifying the Destination (PKCS#12)

You can select any one of the following destination for the X.509 Format:

- Remote System—To export the certificates and private keys to a remote server using TFTP, FTP, SCP, or RCP.
- Redundant SSLSM—To export the certificates and private keys to a redundant SSL services module.

Specify Destination Details (PKCS#12 - Remote System)

Specify the details of the Remote system where you want the certificates and private keys to be exported.

The following fields are displayed:

Fields	Description
File Server	
Protocol	Select from options: <ul style="list-style-type: none"> • FTP • RCP • SCP • TFTP
Server IP Address	IP address of the system.
Username	Enter the user name
Password	Enter the password.
Files	
Directory	Enter the path or location of the files.
SSL Certificate Subject	Displays the list of SSL Certificate Subject.
PKCS#12 File	Displays the list of PKCS#12 Files.

To edit the PKCS#12 files, select the row in the table and click **Edit**.

Click **Next** to continue.

Specify Destination Details (PKCS#12 - Redundant SSLSM)

You can export certificates to a redundant SSLSM. The Wizards will use the same Trustpoint name as the selected Trustpoint on the redundant SSLSM. You can edit the names if required.

You need to specify a staging area. The certificates are exported to the staging area and then imported to the redundant SSLSM from the staging area.



Note

Do not specify a Trustpoint name that already exists in the redundant SSLSM. If the Trustpoint name is already present, the export will fail.

Field	Description
Redundant SSLSM	
IP Address	Enter the IP address.
Username	Enter the user name.
Password	Enter the password.
Enable Username	Re-enter the user name to confirm the user.
Enable Password	re-enter password to confirm.
Remote File Server	
Protocol	Select from the options below: <ul style="list-style-type: none"> • FTP • RCP • SCP • TFTP
Server IP Address	Enter the server IP address.
Username	Enter the user name.
Password	Enter the password.
Files and Trustpoints	
Directory	Enter the path or location of the files.
SSL Certificate Subject	Displays the list of SSL certificate subject names.
PKCS#12 File	Displays the list of PKCS#12 files.
Redundant SSLSM Trustpoint	Displays the list of SSLSM trustpoints that are redundant.

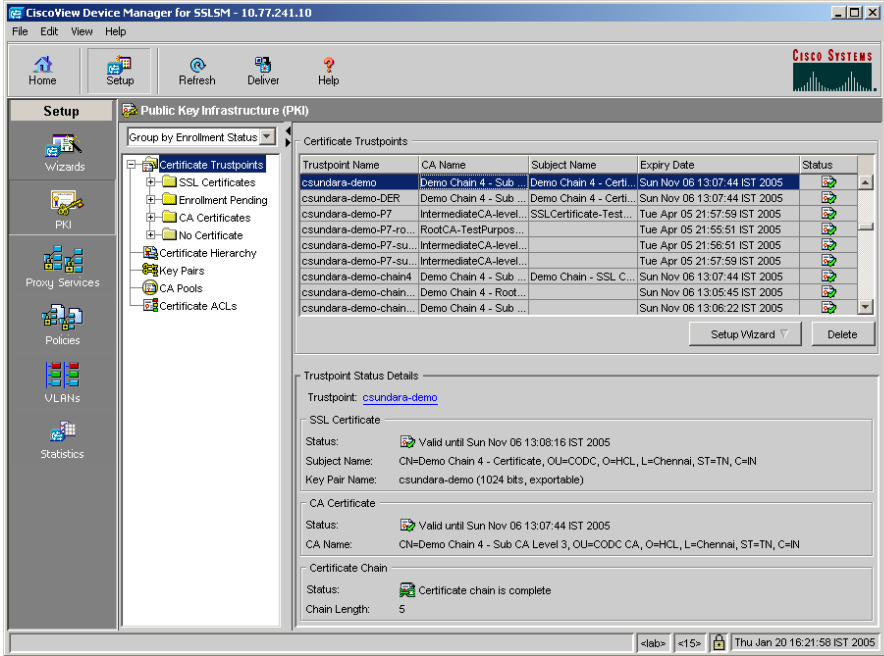
To edit the PKCS#12 files and Redundant SSLSM Trustpoints, select the SSL Certificate Subject in the table and click **Edit**.

Click **Next** to continue.

Viewing Certificate Trustpoints

The Certificate Trustpoint page shows all certificate Trustpoints configured on the SSL Services Module.

Figure 3-2 Public Key Infrastructure Page








To view all Trustpoints:






- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**.

130165

The following information is displayed for Trustpoints:

Field	Description
Trustpoints	
Trustpoint Name	The name of the trustpoint associated with the key pair.
CA Name	Certificate Authority associated with the Trustpoint.
Subject Name	Subject name in the SSL certificate associated with the Trustpoint
Expiry Date	The expiry date of SSL certificate or CA certificate which ever expires earlier
Status	<p>Status of the associated CA certificate.</p> <p>A  icon indicates that the certificate is valid.</p> <p>A  icon indicates that the certificate is invalid.</p> <p>A  icon indicates that the certificate is valid only for less than 10 days.</p> <p>A  icon indicates that the certificate is valid only for less than 20 days.</p> <p>A  icon indicates that the certificate is valid only for less than 30 days.</p> <p>Status will be displayed only for Trustpoints with Certificates.</p>

Select a Trustpoint name from the table to view the following Trustpoint status details.

Field	Description
Trustpoint	The trust point name. Click on the link to view details on the trustpoint.
CA Certificate	
Status	<p>Status of the CA certificate.</p> <p>A  icon indicates that the certificate is valid.</p> <p>A  icon indicates that the certificate is invalid.</p> <p>A  icon indicates that the certificate is valid only for less than 10 days.</p> <p>A  icon indicates that the certificate is valid only for less than 20 days.</p> <p>A  icon indicates that the certificate is valid only for less than 30 days.</p>
CA Name	Subject of the CA Certificate.
SSL Certificate	
Status	Status of the SSL certificate.
Subject Name	Subject of the SSL certificate.
Keypair Name	Key pair to which the trustpoint is associated.
Certificate Chain	
Status	Status of the certificate chain.
Chain Length	Number of certificates in a chain.

You can launch wizards to configure a Trustpoint. To launch the wizard, click **Setup Wizard**, then select one of the following options:

- Configure a Certificate Trustpoint...
- Import Certificates from External PKI...

Select a Trustpoint, then click **Delete** to delete a trustpoint.

Certificate Trustpoint Grouper

You can group Trustpoints based on different common parameters.

To group the Trustpoints:

Step 1 Select one of the options:

- **Group by Enrollment Status**—to group Trustpoints based on the enrollment status. The Trustpoints are displayed under the following groups.
 - SSL Certificates—all Trustpoints that have an SSL Certificate.
 - Enrollment Pending—all Trustpoints that have a CA certificate and key pair configured but do not have an SSL certificate.
 - CA Certificates—all Trustpoints that have a CA certificate configured but the key pair is not configured. All the CA Trustpoints will be grouped under this group.
 - No Certificates—all Trustpoints that do not have any certificate associated with it.
- **Group by Expiry**—to group Trustpoints based on the expiry date. The Trustpoints are displayed under groups starting with the Trustpoints expiring this month, then next month and so on.

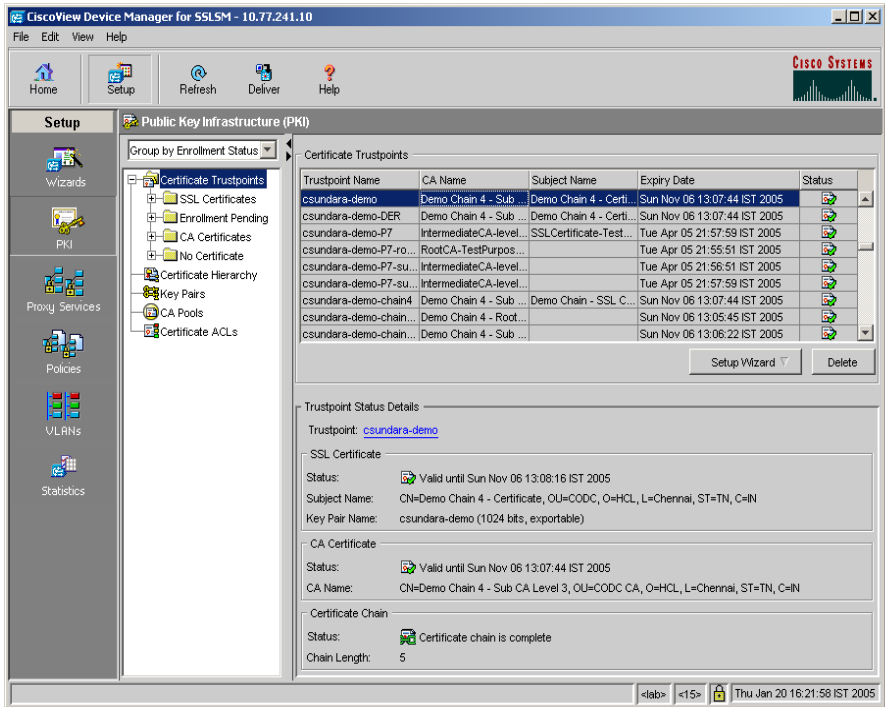
- **Group by CA**—to group Trustpoints by CA.
- **No Grouping**—to list all Trustpoints without any group.

Based on your selection, Trustpoints are grouped under the Trustpoints node in the object [Selector](#).

Certificate Trustpoint Details

You can view the configuration and certificate details of a selected Trustpoint.

Figure 3-3 Public Key Infrastructure Details



130165

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints** from the object **Selector**. The Trustpoint page appears.
- Step 2** Select a Trustpoint object from the logical group. You can group the Trustpoints using Trustpoint Grouper. For more on Certificate Trustpoint Grouper, see [Certificate Trustpoint Grouper, page 3-57](#).
- Step 3** Click **Configuration Tab**.

The following fields are displayed:

Field	Description
Trustpoint Name	The name of the Trustpoint.
Key Pair Name	The key pair associated with the trustpoint.
Certificate	
Subject	The subject of the certificate.
IP Address	The IP address of the module.
Certificate Purpose	The purpose of the certificate.
Include SSL Serial Number in Subject Name	Select this option to include the SSLSM serial number in the subject name.
Enrollment	
Enrollment Method	The enrollment method for the certificate. <i>Example: copy-and-paste.</i>
CA Server URL	The URL of the CA server.
Retry Count	Specifies how many time CVDM should try to enroll the certificate with the module.
Retry Period (min)	Duration between retries, in minutes.
Enable Auto-enrollment	Indicates whether auto-enrollment is enabled for the certificate.
Regenerate keys on auto enrollment	Indicates whether the certificate regenerates keys on autoenrollment.

Field	Description
CRL	
x 500 CDP Information	x500 CDP information for the certificate trustpoint.
CRL Validation	<p>Effectiveness with which the CRL has to be validated.</p> <p>Values are:</p> <ul style="list-style-type: none"> • Default—If the trustpoint has been selected to validate a certificate. If the CRL is not in the database or has expired, the SSL module downloads a CRL and saves it to the database for later use. If the CRL download fails, the SSL module rejects the certificate being validated. • Optional— If the SSL module finds a CRL in the database and has not expired, then the SSL module performs a CRL lookup. If the SSL module does not find CRL, the SSL module accepts the certificate. The SSL module makes no attempt to download a CRL. • Best-effort—If the SSL module finds a CRL in the database and has not expired, then the SSL module performs a CRL lookup. If the SSL module does not find CRL, the SSL module attempts to download a CRL. However, if the CRL download fails, the SSL module accepts the certificate.



Field	Description
Certificate ACL	
Certificate ACL	The name of the Certificate ACL associated with the Trustpoint.

To view SSL certificate details, click **SSL Certificate** Tab.

To view CA Certificate details, click **CA Certificate** Tab.

To view Certificate chain details, click **Certificate Chain** Tab. The certificate chain is displayed in tree format. Each node displays the subject of the certificate.

You can view the details of each certificate on the chain. The following fields are displayed:

Field	Description
Status	<p>Indicates the status of the selected certificate chain.</p> <p>A  icon indicates that the certificate chain is complete.</p> <p>A  icon indicates that the certificate chain is incomplete.</p> <p>Example: Certificate chain is complete - CA certificate is the Root.</p>
Certificate Details	
Certificate	<p>Shows the details of the certificate including the details on how long the certificate is valid.</p> <p>Other details include:</p> <ul style="list-style-type: none"> • Version and serial number • Issuer • Subject • Subject Public Key Information

Field	Description
Associated Trustpoint	Click on the link to view the Trustpoint details.
Trustpoint name	The name of the trustpoint associated with the certificate.

Click **Operations** and select any one of the following Trustpoint operations:

Trustpoint Operation	Description
Authenticate	<p>Select this option to authenticate a CA certificate. You must configure the enrollment method for the Trustpoint to perform this operation.</p> <p>For more information on authenticating a Trustpoint, see Authenticating Trustpoints, page 3-65</p>
Enroll	<p>Select this option to create a certificate request. You must configure the enrollment method and key pair to perform this operation.</p> <p>For manual enrollment methods (Copy and Paste/TFTP) a certificate request will be created. For SCEP enrollment, the certificate request will be sent to the CA server.</p> <p>For SCEP enrollment, you must configure a Challenge Password. If password is not configured, a challenge password dialog box will appear.</p> <p>For more information on authenticating a Trustpoint, see Enrolling Trustpoints, page 3-65</p>

Trustpoint Operation	Description
Authenticate and Enroll	<p>Select this option to authenticate a CA certificate and create a certificate request. For manual enrollment (Copy and Paste/TFTP) a certificate request will be created. For SCEP enrollment, the certificate request will be sent to the CA server.</p> <p>You must configure enrollment method and key pair for the Trustpoint to perform this operation.</p> <p>For SCEP enrollment, you must configure a Challenge Password. If password is not configured, a challenge password dialog box will appear.</p> <p>For more information on authenticating a Trustpoint, see Authenticating and Enrolling Trustpoints, page 3-66</p>
Import SSL Certificate	<p>Select this option to import an SSL certificate issued by the CA for manual enrollment (Copy and Paste/TFTP).</p> <p>For more information on authenticating a Trustpoint, see Importing SSL Certificate Trustpoints, page 3-66</p>

Trustpoint Operation	Description
Renew	<p>Select this option to create a new certificate request. You can optionally regenerate the keys when creating the certificate request.</p> <p>For manual enrollment methods, a certificate request will be created. For SCEP enrollment, the certificate request will be sent to the CA server.</p> <p>This option is enabled only for Trustpoints with SSL certificate.</p> <p>For more information on authenticating a Trustpoint, see Renewing Trustpoints, page 3-67</p>
Export	<p>Select this option to export the certificate and private key associated with the Trustpoint. You can export the certificate only if the private key is exportable.</p> <p>For more information on authenticating a Trustpoint, see Exporting Trustpoints, page 3-68</p>

To edit the Trustpoint configuration, click **Edit**. For more information on editing Trustpoints, see [Editing Trustpoint Configuration, page 3-68](#)

Authenticating Trustpoints

The Trustpoint Authentication dialog box provides the authentication details and the status.

To authenticate a trustpoint, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. You can group the Trustpoints using Trustpoint Grouper. The Trustpoint details dialog box appears with the configuration information.
 - Step 3** Click **Operations**, then select **Authenticate**. The Authentication dialog box appears.
-

Enrolling Trustpoints

To enroll a certificate trustpoint, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. You can group the Certificate Trustpoints using Grouper. The Trustpoint details dialog box appears with the Configuration information.
 - Step 3** Click **Operations**, then select **Enroll**.
-

Authenticating and Enrolling Trustpoints

To authenticate and enroll a certificate trustpoint, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. You can group the Certificate Trustpoints using Grouper. The Trustpoint details dialog box appears with the Configuration information.
 - Step 3** Click **Operations**, then select **Authenticate and Enroll**.
-

Importing SSL Certificate Trustpoints

To import a SSL Certificate, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. You can group the Certificate Trustpoints using Grouper. The Trustpoint details dialog box appears with the Configuration information.
 - Step 3** Click **Operations**, then select **Import SSL Certificate**.
-

Renewing Trustpoints

To renew a certificate trustpoint, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. You can group the Certificate Trustpoints using Grouper. The Trustpoint details dialog box appears with the Configuration information.
 - Step 3** Click **Operations**, then select **Renew**. The Trustpoint Operation - Renew popup dialog box appears with the following fields:

Field	Description
Regenerate	Select the check box to regenerate the certificate.
Keypair Name	Name of the key pair.
Usage	Describes the use of the key. Example: General Purpose.
Key Size (bits)	Size of the key in bits.
Exportable	Indicates whether you can export the key.

- Step 4** Click **OK** to make changes.
-


Exporting Trustpoints


To export a SSL Certificate, do the following:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**. The Trustpoint page appears.
- Step 2** Select a Trustpoint object from the logical group. You can group the Certificate Trustpoints using Grouper. The Trustpoint details dialog box appears with the Configuration information.
- Step 3** Click **Operations**, then select **Export SSL Certificate**.
-

Editing Trustpoint Configuration

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints** from the object **Selector**.
- Step 2** Select a Trustpoint from the table, then click **Edit**. The Trustpoint Edit dialog box appears with the following fields:

Field	Action/Description
General	
Trustpoint Name	Name of the Trustpoint.
Key Pair Name	<p>Name of the key pair associated with the Trustpoint.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> • Create and use a new Key Pair • Select an existing Key Pair • Regenerate Key Pair • Clear the Key Pair

Field	Action/Description
Certificate Purpose	Select the purpose of the certificate from the list: <ul style="list-style-type: none"> • ssl-client • ssl-server
Enrollment Configuration	
Enrollment Method	Select one of the following certificate enrollment method: <ul style="list-style-type: none"> • SCEP • TFTP • Copy and Paste
CA Server URL	Enter the enrollment URL of the certification authority server.
Retry Count	Enter the number of retries.
Retry Period	Enter the interval between the retries.
HTTP Proxy	Enter the IP address of the HTTP proxy.
Port	Enter the port number for the HTTP proxy.
Auto Renewal and Enrollment	Select the checkbox to enable auto renewal and enrollment.
Renewal Percentage (%)	Enter the percentage of renewal. Default is 100%.
Challenge Password	Enter the Challenge Password . Click  and select one of the following options: <ul style="list-style-type: none"> • Configure a Challenge Password • Clear Challenge Password
Regenerate Keys on Re-enrollment	Select this checkbox to regenerate key on re-enrollment.
CRL Configuration	

Field	Action/Description
x.500 CDP Information	<p data-bbox="803 238 1188 266">Enter the X.500 CDP information.</p> <p data-bbox="803 285 1233 410">You can enter the hostname and port if the CDP is in X.500 DN format. The query takes the information in the following form: ldap://hostname:[port]</p> <p data-bbox="803 427 1184 487">For example, if a certificate being validated has the following:</p> <ul data-bbox="817 503 1228 670" style="list-style-type: none"> <li data-bbox="817 503 1228 563">• The X.500 DN is configured with CN=CRL,O=Cisco,C=US <li data-bbox="817 579 1228 670">• The associated trustpoint is configured with crl query ldap://10.1.1.1 <p data-bbox="803 686 1200 747">then the two parts are combined to form the complete URL as follows:</p> <p data-bbox="803 763 1228 823">ldap://10.1.1.1/CN=CRL,O=Cisco,C=US.</p> <p data-bbox="803 839 1228 1125">Note The trustpoint should be associated with the issuer certificate authority certificate of the certificate being validated. If there is no such trustpoint in the database, the complete URL cannot be formed, and CRL download cannot be performed.</p>

Field	Action/Description
CRL Validation	<p>Select the type of CRL validation to be used for the certificate:</p> <ul style="list-style-type: none"> • Default—If the trustpoint has been selected to validate a certificate. If the CRL is not in the database or has expired, the SSL module downloads a CRL and saves it to the database for later use. If the CRL download fails, the SSL module rejects the certificate being validated. • Optional— If the SSL module finds a CRL in the database and has not expired, then the SSL module performs a CRL lookup. If the SSL module does not find CRL, the SSL module accepts the certificate. The SSL module makes no attempt to download a CRL. • Best-effort—If the SSL module finds a CRL in the database and has not expired, then the SSL module performs a CRL lookup. If the SSL module does not find CRL, the SSL module attempts to download a CRL. However, if the CRL download fails, the SSL module accepts the certificate.
Certificate ACL	
Certificate ACL	Enter the Certificate ACL information.

Step 3 Modify the values, then click **OK**.

Selecting Available ACLs

The following information appears:

Field	Action/Description
Certificate ACLs	The name of the certificate ACL.

Select ACLs from the table, then click **OK**.

Selecting Available Key Pairs

The following information appears:

Field	Action/Description
Key Pair Name	The name of the key pair.
Key Size	The size of the key pair.

Select key pairs from the table, then click **OK**.

Certificate Hierarchy

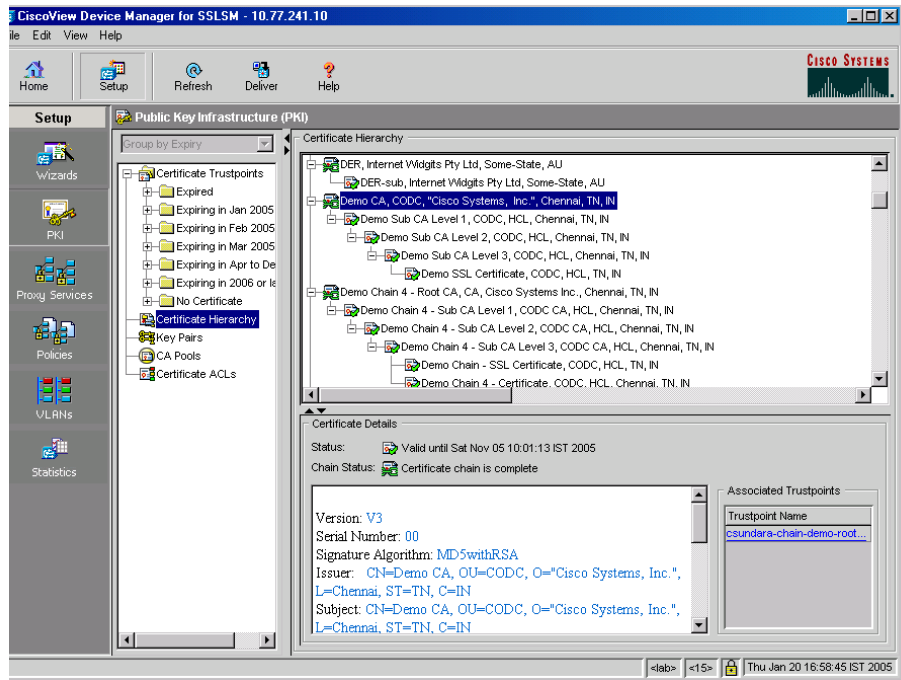
Certificate Hierarchy helps you to browse through the certificates imported on the SSLSM and visualize the certificate hierarchy. You can also see the validity status and the certificate chain status in the certificate tree.

In the Associated Trustpoints table, you have the hyperlinks to the associated Trustpoints. You can view and configure the trustpoints by clicking the hyperlink.

To view the Certificate Hierarchy:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Hierarchy** from the object **Selector**. The certificate tree appears in the content pane.
 - Step 2** Select a certificate from the certificate hierarchy tree. The details of the selected certificate is displayed in the Certificate Details box and the associated Trustpoint names appears in the Associated Trustpoint box.
-

Figure 3-4 PKI > Certificate Hierarchy Page



130164

Deleting Certificates

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints** from the object **Selector**.
- Step 2** Select a Trustpoint from the table.
- Step 3** Click **Delete**.

Challenge Password

Challenge password is required for SCEP enrollment. If you have not configured a challenge password, challenge password dialog will be prompted.

This password is necessary in the event that you ever need to revoke your certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

The Challenge Password dialog box has got two fields. Challenge Password and Confirm Password. Enter the password and confirm it. Click **OK** to continue.

How Do I...

This section describes on how to achieve a task. The following questions are answered:

- [How Do I Import an SSL Certificate and Private Key to SSLSM?, page 3-76](#)
- [How do I Import a CA Certificate Chain on the SSLSM?, page 3-77](#)
- [How do I generate a Certificate Signing Request \(CSR\)?, page 3-78](#)
- [How do I import the SSL certificate obtained using CSR?, page 3-81](#)
- [How Do I Export Certificates and Private Keys from SSLSM?, page 3-82](#)
- [How Do I Renew an SSL Certificate?, page 3-82](#)

How Do I Import an SSL Certificate and Private Key to SSLSM?

The Certificate Import Wizard helps you to import the SSL certificate and the private key on the SSLSM. If you are importing the SSL certificate and private key from your client machine, you could also import the associated CA certificate chain.

-
- Step 1** Click **Setup** in the CVDM-SSLSM task bar. The Setup page appears.
- Step 2** Click **Wizards** in the left-most pane. The Setup Wizard page appears.
- Step 3** Select **Import Certificates and Private key**, then click **Launch the Selected Task**. The Certificate Import Wizard appears.

You can import files in any of the following format:

- PKCS#12
- X.509 PEM
- X.509 DER
- PKCS#7

**Note**

When creating a PKCS#12 file, include the entire certificate chain, from server certificate to root certificate, and public and private keys. You can also generate a PKCS#12 file from the module and export it.

**Note**

If you are using SSH, we recommend using SCP when importing or exporting a PKCS#12 file. SCP authenticates the host and encrypts the transfer session.

For details on Certificate Import Wizard, see [Import Certificates and Private Key, page 3-4](#).

How do I Import a CA Certificate Chain on the SSLSM?

The Certificate Trustpoint Setup Wizard helps you to Import a CA certificate chain.

To configure a certificate Trustpoint:

-
- Step 1** Click **Setup** in the task bar. The Setup page appears.
 - Step 2** Click **Wizard** in the left-most pane. The Wizards information page appears.
 - Step 3** Click the **Certificate Wizards**. The Certificate Wizards page appears.
 - Step 4** Select **Configure a Certificate Trustpoint**, then click **Launch the Selected Task** to launch the wizard.
-

You could Import a CA certificate chain using CA certificates in X.509 Privacy Enhanced Mail (PEM) format or PKCS#7 format.

Importing a CA certificate chain in PEM format

To import a CA certificate chain using CA certificates in PEM format, you need to perform the following tasks:

-
- Step 1** Specify a Trustpoint name prefix. When importing a certificate chain, a CA certificate Trustpoint is setup for each of the CA certificates in the certificate chain. Select the **CA Trustpoint**.
 - Step 2** Select X.509 PEM from the format options, select the source from which you wish to import the CA certificates and select the **Import a CA Certificate Chain** option.
 - Step 3** Specify the CA certificates in the certificate chain. You must specify the CA certificates starting from the root CA certificate (self-signed certificate) to your subordinate CA. A Trustpoint name is automatically generated for the CA Trustpoints based on the prefix specified in Step 1. You can edit the Trustpoint names using the CA Trustpoints tab. Importing a CA certificate chain in PKCS#7 format

Review the summary and click **Finish**. A status dialog will be launched displaying the status of the certificate Trustpoint setup.

To import a CA certificate chain in PKCS#7 format, perform the following tasks:

-
- Step 1** Specify a Trustpoint name prefix. When importing a certificate chain, a CA certificate Trustpoint will be setup for each of the CA certificates in the certificate chain. Select the **CA Trustpoint**.
- Step 2** Select PKCS#7 from the format options. To import a PKCS#7 file from your client machine select the **Local Hard Disk** option and specify the PKCS#7 file. The wizard will decode the PKCS#7 file and list all the CA certificates in the file. A default Trustpoint name is automatically generated for each of the CA certificates based on the Trustpoint name prefix specified in Step 1. You can double-click on the row to edit the Trustpoint name.
- Step 3** Specify the CA certificates in the certificate chain. You must specify the CA certificates starting from the root CA certificate (self-signed certificate) to your subordinate CA. A Trustpoint name will be automatically generated for the CA Trustpoints based on the prefix specified in Step 1. You can edit the Trustpoint names using the CA Trustpoints tab.

Review the summary and click **Finish**. A status dialog will be launched displaying the status of the certificate Trustpoint setup.

How do I generate a Certificate Signing Request (CSR)?

To generate a Certificate Signing Request (CSR), do the following tasks:

- If the Certificate Authority (CA) issuing your SSL certificate is a subordinate CA, import all the CA certificates in the certification path. If your CA is a root CA (self-signed CA certificate), you can skip this task.
- Configure a certificate Trustpoint, authenticate the CA certificate corresponding to the issuer of your SSL certificate, and generate a CSR.

The Certificate Trustpoint Setup Wizard helps you perform the above tasks.

Importing a CA certificate chain



Note

If the issuing CA certificate is a self-signed certificate, you can skip this step.

For more details, see [How do I Import a CA Certificate Chain on the SSLSM?](#)

Configuring a Certificate Trustpoint

To configure a certificate Trustpoint:

-
- Step 1** Click **Setup** in the task bar. The Setup page appears.
 - Step 2** Click **Wizard** in the left-most pane. The Wizards information page appears.
 - Step 3** Click the **Certificate Wizards**. The Certificate Wizards page appears.
 - Step 4** Select **Configure a Certificate Trustpoint**, then click **Launch the Selected Task** to launch the wizard.
 - Step 5** Specify a Trustpoint name and select the **Proxy Service Trustpoint** option. By default, a new RSA key pair will be generated with the same name as the Trustpoint. Specify the key size. If you already have the RSA key pair on the SSLSM, select the **Use an Existing Key Pair** option and specify the key pair name.
 - Step 6** Specify the certificate attributes - subject Distinguished Name (DN), unstructured name, unstructured IP address and, certificate purpose. These attributes are optional.
 - Step 7** Specify the enrollment method. SSLSM supports three methods of certificate enrollment.

- **Automatic Enrollment using Simple Certificate Enrollment Protocol (SCEP)**

If SCEP is used, SSLSM sends the certificate request (CSR) to the specified SCEP server. The SSL certificate issued by the CA is automatically imported.

- **Manual Enrollment using TFTP**

In this method, you must specify a filename on your TFTP server.

For example,
`tftp://10.77.241.10/certs/mycert`

SSLSM adds file extensions to the filename as follows:

- `.ca` when downloading the CA certificate from the TFTP server.

For example `mycert.ca`

- `.req` when copying the generated CSR to the TFTP server.

For example `mycert.req`

- `.crt` when downloading the SSL certificate from the TFTP server.

For example `mycert.crt`

- **Manual Enrollment using Copy-and-Paste**

In this method, the CSR is displayed to you. You can copy the CSR and submit it to your CA.

If certificate Trustpoints exists on the SSLSM, and are enrolled with CAs, the CA field lists the corresponding CA names. If you select a CA, the corresponding enrollment configuration is applied to the new Trustpoint.

Step 8 Specify the CA certificate

This step applies only to Copy-and-Paste method. When using the copy-and-paste method, you must specify the certificate of your CA issuing the SSL certificate.

For TFTP method, the SSLSM will download the CA certificate from the TFTP server.

Step 9 Select **Authenticate the CA and Generate a CSR** option from the setup task options and click Next.

Review the summary and click Finish. A status dialog will be launched displaying the status of the certificate Trustpoint setup.

When authenticating the CA certificate, the MD5 fingerprint of the CA certificate will be displayed. You need to manually verify the fingerprint and accept the certificate. For copy-and-paste method, the CSR will be displayed. For TFTP method, the CSR will be copied to the TFTP server.

How do I import the SSL certificate obtained using CSR?

Importing SSL Certificate using Certificate Trustpoint Setup Wizard

If you are using TFTP enrollment method, copy the SSL certificate obtained using the CSR to the TFTP server. You must use the filename configured in the Trustpoint with a.crt file extension.

-
- Step 1** Specify the name of the certificate Trustpoint that you setup to generate the CSR.
 - Step 2** Skip this step.
 - Step 3** Skip this step.
 - Step 4** Select **Import SSL Certificate** from the setup task option.
 - Step 5** This step applies only if you are using copy-and-paste enrollment method. Copy and paste the SSL certificate in PEM format.
- Review the summary and click **Finish**. A wizard status dialog will be launched displaying the status of the SSL certificate import.
-

Importing SSL Certificate from Trustpoint Details Screen

To import a SSL Certificate, do the following:

-
- Step 1** Click **Setup** at the top of the window, click PKI in the left-most pane, and select **Certificate Trustpoints** from the object [Selector](#). The Trustpoint page appears.
 - Step 2** Select a Trustpoint object from the logical group. The Trustpoint details screen appears with the Configuration information.
 - Step 3** Click **Operations**, then select **Import SSL Certificate**.
- Review the summary and click **Finish**. A wizard status dialog will be launched displaying the status of the SSL certificate import.
-

How Do I Export Certificates and Private Keys from SSLSM?

The Certificate Export Wizard helps you to export the SSL certificate and the private key from the SSLSM. If you are exporting the SSL certificate and private key to your client machine, you could also export the associated CA certificate chain.

For details of Certificate Export Wizard, see [Export Certificates and Private Keys](#), page 3-7.

How Do I Renew an SSL Certificate?

You can renew Certificates and Key pairs.

-
- Step 1** Click **Setup** at the top of the window, click PKI in the left-most pane, and select Trustpoints from the object [Selector](#). The Trustpoint page appears.
 - Step 2** Select a Trustpoint node from the logical group. You can group the Trustpoints using Trustpoint Grouper.
 - Step 3** Select a **Trustpoint** from the list.
 - Step 4** Click Operations, then select **Renew** from the popup menu.

Review the summary and click Finish. A status dialog will be launched displaying the status of the certificate Trustpoint setup.



Managing Key Pairs

The following topics are described in this section:

- [Understanding Key Pairs, page 4-1](#)
- [Viewing Key Pairs, page 4-2](#)
- [Adding Key Pairs, page 4-4](#)
- [Deleting Key Pairs, page 4-6](#)
- [Key Pair Wizard, page 4-6](#)
- [How Do I..., page 4-16](#)

Understanding Key Pairs

RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Aldeman. RSA algorithm is widely used by certificate authorities and SSL servers to generate key pairs. Each certificate authority and each SSL server has its own RSA key pair. The SSL server sends its public key to the certificate authority when enrolling for a certificate. The SSL server uses the certificate to prove its identity to clients when setting up the SSL session.



Note

The SSL Services Module supports only general-purpose keys.

When you generate general-purpose keys, only one pair of RSA keys is generated. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate. We recommend that you specify a name for the key pairs.

When you generate RSA keys, you are prompted to enter a modulus length in bits. The SSL Services Module supports modulus lengths of 512, 768, 1024, 1536, and 2048 bits. Although you can specify 512 or 768, we recommend a minimum modulus length of 1024. A longer modulus takes longer to generate and takes longer to use, but it offers stronger security.

Viewing Key Pairs

The Key Pairs page shows all key pairs configured on a Trustpoint.

To view all Key Pairs:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane.
- Step 2** Select **Trustpoints > Key Pairs** from the object selector.

The following information is displayed for Key Pairs:

Field	Description
Name	Name associated with the Key pair.
Key Size	Size of the keys in bits. Choose the size of the key modulus from the list. Supported key sizes are: <ul style="list-style-type: none"> • 512 • 768 • 1024 • 1536 • 2048
Usage	The purpose of the key. Only general purpose keys are supported by the SSLSM.

Field	Description
Generation / Import Time	The time when the key pair was generated or imported to the SSLSM.
Exportable	<p>Check box indicating if the key pair can be exported.</p> <p>You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.</p>

Select a key pair to view details. The following details are displayed at the lower part of the content window:

Key Pair Details

Field	Description
General	
Key Pair Name	Name associated with the Key pair
Key Size (bits)	Size of the keys in bits.
Usage	The purpose of the key. Only general purpose keys are generated by the SSLSM.
Generation/Import Time	The time when the key pair was generated or imported to the SSLSM.
Exportable	<p>Check box indicating if the key pair can be exported or not.</p> <p>You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.</p>

Associated Trustpoints

Field	Description
Trustpoint Name	The names of the Trustpoints to which the key pair is associated.
Subject Name	Subject name of the certificate using the key.
Public Key	The hexadecimal value of the public key.

Click **Add** to add a new key pair.

Select a key pair from the table, then click **Delete** to delete a key pair.

Click **Import** to launch the Key Pair Import Wizard.

Click **Export** to launch the Key Pair Export Wizard.

Adding Key Pairs

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane.
 - Step 2** Select **Trustpoints > Key Pairs** from the object selector.
 - Step 3** Click **Add**. **Add New Key Pair** dialog box appears.
 - Step 4** Modify the appropriate values.

Field	Description
Key Pair Name	Name associated with the Key pair.
Usage	The purpose of the key.
Key Size (bits)	Size of the keys in bits Choose the size of the key modulus from the list. Supported key sizes are: <ul style="list-style-type: none">• 512• 768• 1024• 1536• 2048.
Exportable	Checkbox indicating if the key pair can be exported. You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.

Deleting Key Pairs

You can delete key pairs. Deleting a key pair will delete all Certificates issued using the selected keys.

To delete key pairs:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane. elect **Trustpoints > Key Pairs** from the object selector.
 - Step 2** Click **Delete**. Key Pair Deletion confirmation box appears.
 - Step 3** Click **Yes** to delete the key pair.
-

Key Pair Wizard

You can import and export key pairs in privacy-enhanced mail (PEM) file format. The Key Pair Wizard allows you to import and export key pairs.

- [Key Pair Import Wizard, page 4-7](#)
- [Key Pair Export Wizard, page 4-10](#)

Key Pair Import Wizard

The Key Pair wizard allows you to import RSA Key pairs in PEM format to SSLM.

To import a Key Pair:

-
- Step 1** Specify Key Pair Name and Source.
 - Step 2** Specify Public and Private Keys.
 - Step 3** Click **Finish**.
-

Specify Key Pair Name and Source

This page of the key pair import wizard allows you to enter key pair name and the source from where the key pair has to be imported.

The following fields are displayed:

Field	Action/Description
Key Pair Name*	The name of the key pair.
Allow Key Pair Export	Select the check box if you want to allow key pair export. You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.
Local Hard Disk	Select this if you are importing key pair from a local hard disk.
Copy and Paste	Select this if you are using copy and paste to import the key pairs.
Remote System	Select this if you are importing from a remote system.

Public and Private Keys (Local Hard Disk)

If you select **Local Hard Disk**, the following fields appear:

Field	Description
Public Key File	The public key file you need to export. Enter the absolute path or browse and select the file from the local hard disk.
Private Key File	The private key file you need to export. Enter the absolute path or browse and select the file from the local hard disk.
Passphrase	The passphrase to be used to encrypt the key.

Public and Private Keys (Copy-and-Paste)

If you select **Copy-and-Paste**, the following fields appear:

Field	Description
Public Key	Copy-and-paste the public key here.
Passphrase	The passphrase that is used to protect the private key. The passphrase can be any phrase including spaces and punctuation except for question mark (?). Passphrase protection associates a passphrase to the key. The passphrase is used to encrypt the key when it is exported. When the key is imported, you must enter the same passphrase to decrypt it.
Private Key	Copy-and-paste the private key.

Public and Private Keys (Remote System)

If you select **Remote System**, the following fields appear:

Field	Description
Protocol	The protocol to used for the transfer.
IP Address	The IP address of the Remote System.
User Name	The user name.
Password	Password
Public Key File Name	The absolute path of the public key file.
Private Key File Name	The absolute path of the public key file.
Passphrase	<p>The passphrase that is used to protect the private key.</p> <p>The passphrase can be any phrase including spaces and punctuation except for question mark (?). Passphrase protection associates a pass phrase to the key. The passphrase is used to encrypt the key when it is exported. When the key is imported, you must enter the same pass phrase to decrypt it.</p>

Key Pair Export Wizard

The Key Pair Export Wizard allows you to export an RSA key pair in PEM format.

You can export key pairs to a local hard disk or a remote system. Alternatively you can copy-and-paste the key pair values.

To export key pairs:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Key Pairs** from the object selector.
 - Step 2** Select a Key Pair from the table.
 - Step 3** Click **Export**. The Export Key Pair dialog box appears.
 - Step 4** Select a **Destination** type.
 - Step 5** Specify destination file names and encryption parameters. Fields in the dialog box varies according to the destination type you select.
 - Step 6** Click **Finish** to complete exporting.
-

Key Pair Destination

The Key Pair Destination page of the wizard allows you to select the key pair destination.

You can select any one of the destination types:

- Local Hard Disk—to export the keys to a client workstation.
- Copy-and-Paste—to copy-and-paste the public and private keys.
- Remote System—to export the keys to a remote system using TFTP, FTP, SCP, or RCP.

If you have selected Local Hard disk, next step is to specify [Destination Files and Encryption Parameters \(Local Hard Disk\)](#), page 4-11.

If you have selected Copy-and-paste, next step is to specify [Encryption Parameters \(Copy-and-paste\)](#), page 4-13.

If you have selected Remote System, next step is to specify [Destination Files and Encryption Parameters \(Remote System\)](#), page 4-14.

Destination Files and Encryption Parameters (Local Hard Disk)

The Destination Files and Encryption Parameters page of the wizards allows you to enter the destination files names of the public and private key on the client station, and encryption parameters.

If you select **Local Hard Disk** the following fields appear:

Field	Description
Public Key File	The public key file you need to export. Enter the absolute path or browse and select the file from the local hard disk.
Private Key File	The private key file you need to export. Enter the absolute path or browse and select the file from the local hard disk.
Encryption	The encryption to used for the key pair. The following encryption algorithms are supported: <ul style="list-style-type: none">• des—Specifies the 56-bit DES-CBC encryption algorithm.• 3des—Specifies the 168-bit DES (3DES) encryption algorithm.

Field	Description
Passphrase	<p>The passphrase that is used to protect the private key.</p> <p>The passphrase can be any phrase including spaces and punctuation except for question mark (?).</p> <p>Passphrase protection associates a passphrase to the key. The passphrase is used to encrypt the key when it is exported. When the key is imported, you must enter the same pass phrase to decrypt it.</p>
Confirm Passphrase	Confirm the passphrase to decrypt the key pair.

Enter the details, then click **Next**.

Encryption Parameters (Copy-and-paste)

You can enter the encryption type and pass phrase to protect the private key.

The following fields appear:

Field	Description
Encryption	<p>Encryption used by the key pair.</p> <p>The following encryption algorithms are supported:</p> <ul style="list-style-type: none"> des—Specifies the 56-bit DES-CBC encryption algorithm. 3des—Specifies the 168-bit DES (3DES) encryption algorithm.
Passphrase	<p>The passphrase that is used to protect the private key.</p> <p>The passphrase can be any phrase including spaces and punctuation except for question mark (?).</p> <p>Passphrase protection associates a passphrase to the key. The passphrase is used to encrypt the key when it is exported. When the key is imported, you must enter the same pass phrase to decrypt it.</p>
Confirm Passphrase	<p>Confirm the passphrase to decrypt the key pair.</p>

Destination Files and Encryption Parameters (Remote System)

The Destination Files and Encryption Parameters page of the wizards allows you to enter the destination files names of the public and private key on the client station, and encryption parameters.

If you select **Remote System**, the following fields appear:

Field	Description
Protocol	The protocol to used for the transfer.
IP Address	The IP address of the remote system.
User Name	The user name.
Password	Password to be used for the remote system.
Public Key File	The absolute path of the public key file.
Private Key File	The absolute path of the public key file.
Encryption	<p>Encryption used by the key pair.</p> <p>The following encryption algorithms are supported:</p> <ul style="list-style-type: none"> • des—Specifies the 56-bit DES-CBC encryption algorithm. • 3des—Specifies the 168-bit DES (3DES) encryption algorithm.

Field	Description
Passphrase	<p>The passphrase that is used to protect the private key.</p> <p>The passphrase can be any phrase including spaces and punctuation except for question mark (?). Passphrase protection associates a passphrase to the key. The passphrase is used to encrypt the key when it is exported. When the key is imported, you must enter the same pass phrase to decrypt it.</p>
Confirm Passphrase	Confirm the passphrase to used for decrypting the key pair.

Key Pair Wizard Summary

When you use a wizard to perform a configuration, the wizard's Summary screen displays the values that you have configured. You can examine those values and click the wizard's Back button to return to a screen on which you need to make a change. When you have made the changes, click the Finish button to save your changes and leave the wizard.

Key Pair Wizard Status

The Key Pair Wizard Status dialog box provides the status details of the Trustpoint configuration tasks. The details displayed vary according to the task you selected. The dialog box displays the status against each task.

The configuration performed on the module is displayed in the content area. If any task fails, you can review the task details and take necessary action.

How Do I...

The How do I section explains how to accomplish a task using the CVDM.

The following tasks are explained:

- [How Do I Add a New Key Pair?](#)
- [How Do I Import a Key Pair?](#)

How Do I Add a New Key Pair?

To add a new key pair:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane.
 - Step 2** Select **Trustpoints > Key Pairs** from the object selector.
 - Step 3** Click **Add**. Add New Key Pair dialog box appears.
 - Step 4** Modify the appropriate values in the page, the click **OK**.
-

How Do I Import a Key Pair?

You can use the key pair import wizard to import a key pair. The Key Pair wizard allows you to import RSA Key pairs in PKCS12 or PEM format to SSLM.

To import a key pair:

-
- Step 1** Launch the Key Pair Import Wizard.
 - Step 2** Enter key pair name and the source from where the key pair has to be imported.
 - Step 3** Enter the public and private key information.
-



Managing CA Pools

Certification authorities (CAs) are responsible for managing certificate requests and issuing digital certificates. A digital certificate contains information, such as a name, serial number, company, department, or IP address, that identifies a user or device. A digital certificate also contains a copy of the entity's public key. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

CVDM-SSLSM allows you to create trusted CA pools, which lists the CAs that the module can trust. You can select Trustpoints and create pools and assign a CA pool to one or more proxy services.

The following topics are described in this section:

- [Viewing CA Pools, page 5-2](#)
- [Assigning CA Pools to Proxy Services, page 5-4](#)
- [Adding CA Pools, page 5-5](#)
- [Editing CA Pools, page 5-6](#)
- [Deleting CA Pools, page 5-7](#)
- [How Do I..., page 5-7](#)




Viewing CA Pools

You can view information on all CA Pools configured on SSLSM.



To view CA Pools:

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.

This page displays the following fields:

Field	Description
Name	Name of the CA Pool.
Number of Trustpoints	Number of Trustpoints in the Pool.
Number of Proxy Services (Use Count)	Number of Proxy Services using the CA Pool.
Status	Status of the CA Pool. A  icon indicates that all certificates in the CA Pool are valid. A  icon indicates that some certificates in the CA Pool are invalid. A  icon indicates that all certificates in the CA Pool are invalid.

Step 2 Select a CA Pool from the table. The following details are displayed:

Field	Description
Trustpoint Name	The name of the associated Trustpoint.
Status	The status of the associated Trustpoint. A  icon indicates that the certificate is valid. A  icon indicates that the certificate is invalid.
CA Name	The name of the certification authority associated with the Trustpoint.
Associated Proxy Services	
Service Name	Name of service.
Client Side (Virtual)	Virtual IP address and port of the proxy service.

To assign CA Pools to proxy services, select a CA Pool, then click **Assign to Proxy Services....**

To add a new CA Pool, click **Add**.

To edit a CA Pool, select a CA Pool, then click **Edit**.

To delete a CA Pool, select a CA Pool, then click **Delete**.

Assigning CA Pools to Proxy Services

You can select proxy services and assign a CA Pool to the selected proxy service.

To assign CA Pools to proxy services:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.
- Step 2** Select a CA Pool, then click **Assign to Proxy Services**. The **Assign CA Pool to Proxy Services** dialog box appears.

The following fields appear:

Field	Description
Pool Name	Name of the CA Pool.
Proxy Service Name	Name of the Proxy Service.
Client Side (Virtual)	IP address and port of the proxy service.
Selected Proxy Services	The list of selected proxy services.

- Step 3** Select a Proxy Service name from the list, and click **Add>>** to assign the CA Pool to the service. Use **<< Remove** to remove the CA pool from the list of services. Use **Clear All** to remove all the pools from the service.
- Step 4** Click **OK** to complete assigning the CA pool to the selected Proxy Services.
-

Adding CA Pools

You can add new CA Pools and add Trustpoints to the CA pools.

To add CA Pools:

Step 1 Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.

Step 2 Click **Add**. The **Add CA Pool** dialog box appears.

The following fields appear:

Field	Description
Pool Name	Name of the CA Pool.
Trustpoint Name	Name of the Trustpoint.
CA Name	Name of Trust CA Pool.
Pool Members	Members in the select CA Pool.

Step 3 Enter a Pool Name.

Step 4 Select a Trustpoint name from the list, and click **Add>>** to add the Trustpoint to the CA Pool. Use **<< Remove** to remove the trustpoint name from the pool. Use **Clear All** to remove all the members of the pool.

Step 5 Click **OK** to complete adding the CA Pool.

Editing CA Pools

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.
- Step 2** Select a CA Pool from the table, and Click **Edit**. The **Edit CA Pool** dialog box appears.

The following fields appear:

Field	Description
Pool Name	Name of the CA Pool.
Trustpoint Name	Name of the Trustpoint.
CA Name	Name of Trust CA Pool.
Pool Members	Members in the select CA Pool.

- Step 3** Select a Trustpoint name from the available Trustpoints, and click **Add>>** to add the Trustpoint to the CA Pool. Use **<< Remove** to remove the trustpoint name from the pool members. Use **Clear All** to remove all the members of the pool.
- Step 4** Click **OK** to complete editing the CA Pool.

Deleting CA Pools

To delete CA Pools:

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.
 - Step 2** Select a CA Pool from the table, and click **Delete**.
 - Step 3** Confirm delete action. A warning message appears if the selected CA Pool is associated with any Proxy Service.
-

How Do I...

This section describes on how to achieve a task. The following question is answered:

- [How do I add a new CA Pool?](#)

How do I add a new CA Pool?

-
- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > CA Pools** from the object selector. The CA Pools page appears.
 - Step 2** Click **Add**. The **Add CA Pool** dialog box appears.
 - Step 3** Enter a Pool Name.
 - Step 4** Select a Trustpoint name from the list, and click **Add >>** to add the Trustpoint to the CA Pool. Use **<< Remove** to remove the trustpoint name from the pool. Use **Clear All** to remove all the members of the pool.
 - Step 5** Click **OK** to complete adding the CA Pool.
-



Managing Certificate ACLs

Certificates are used to identify an entity (a user or device) and, using fields within the certificate, to associate attributes with that entity. The certificates include several fields that determine whether the entity is authorized to perform a specified action. The Certificate Security Attribute-Based Access Control feature adds a new command, `crypto CA certificate ACL`, and new fields to the certificate that create the certificate-based access control list (ACL).

The certificate-based ACL specifies one or more fields within the certificate and an acceptable value for each specified field. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value:

- equal
- not equal
- contains
- does not contain
- less than
- greater than or equal

If more than one field is specified within a single certificate-based ACL, the tests of all of the fields within the ACL must succeed to match the ACL.

The same field may be specified multiple times within the same ACL.

More than one ACL may be specified. Each ACL will be processed in turn until a match is found or all of the ACLs have been processed.

CVDM-SSLSM allows you to define certificates (Attribute-Based Access Control) / Certificate ACLs based on the peer certificate attributes.

These topics describe usage of certificate-based ACLs in CVDM-SSLSM:

- [Viewing Certificate ACLs, page 6-2](#)
- [Adding Certificate ACL, page 6-5](#)
- [Editing Certificate ACLs, page 6-7](#)
- [Assigning Certificate ACLs to Trustpoints, page 6-4](#)
- [Deleting Certificate ACLs, page 6-9](#)

Viewing Certificate ACLs

You can view all certificate ACLs configured in the device.

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Certificate Trustpoints > Certificate ACLs** from the object selector.

The following fields appear:

Field	Description
Name	Name or tag associated with the Certificate ACL
Number of ACL Entries	Number of ACL entries
Number of Trustpoints (Use Count)	Number of Trustpoints.

To view the details of a certificate ACL, select a certificate ACL from the table. The following details are displayed at the lower section of the content pane:

Field	Description
Certificate ACL Details: <Certificate ACL name>	
Certificate ACL Entries and Criteria	
Sequence	The sequence numbers of the Certificate ACL entries.

Select a certificate ACL entry by selecting the corresponding sequence number to view the details.

Field	Description
Certificate Field	<p>The Certificate Field to be examined for Access Control.</p> <p>The field name is one of the following case-insensitive name strings or a date:</p> <ul style="list-style-type: none"> • subject-name • issuer-name • unstructured-subject-name • alt-subject-name • name • valid-start • expires-on
Match Condition	<p>The following match conditions are supported:</p> <ul style="list-style-type: none"> • Equals (eq) • Not Equals (neq) • Contains (co) • Not Contains (nc) • Less than (lt) • Greater than or Equals (ge)
Match Value	<p>The name or date to test with the logical operator assigned by match criteria.</p>

Select a certificate ACL from the list, then click **Assign to Trustpoints** to assign a certificate ACL to a trustpoint.

Click **Add** to add a certificate ACL.

To edit a certificate ACL, select a certificate ACL and click **Edit**.

To delete a certificate ACL, select a certificate ACL and click **Delete**.

To view Trustpoints associated with a certificate ACL, select a certificate ACL and click **View Associated Trustpoints**.

Assigning Certificate ACLs to Trustpoints

You can view all certificate ACLs configured in the device.

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Certificate ACLs** from the object selector.
- Step 2** Select a Certificate ACL from the list, and click **Assign to Trustpoints**. The Assign to Trustpoint dialog box appears.

The following fields appear:

Field	Description
Certificate ACL Name	The ACL name of the certificate.
Trustpoint Name	The trustpoint associated with the Certificate ACL.
CA Name	The CA name of the associated trustpoint
Subject Name	The subject name of the certificate.
Selected Trustpoints	Trustpoint associated with the certificates.

- Step 3** Select the Trustpoints from the list, and click **Add>>** to assign the certificate ACL. Click **<< Remove** to remove the trustpoint from the selected list.

Viewing Associated Trustpoints

To view the Trustpoints associated with a Certificate ACL:

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Certificate ACLs** from the object selector.
- Step 2** Select a Certificate Map from the table. The Certificate ACL details appear at the lower section of the content window.
- Step 3** Select a sequence from the sequence list, then click **View Associated Trustpoints**.

The following details appear for the associated Trustpoints:

Field	Description
Trustpoint Name	The trustpoint associated with the Certificate ACL.
CA Name	The CA name of the associated trustpoint.
Subject Name	The subject of the associated trustpoint.

Adding Certificate ACL

- Step 1** Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Certificate ACLs** from the object selector. The Certificate ACLs page appears.
- Step 2** Click **Add**. The Add Certificate ACL dialog box appears.

Using this dialog box you can:

- Add a new ACL entry
- Remove an existing ACL entry

- Add new criteria to an existing ACL entry
- Remove criteria from an existing ACL entry.

The dialog box displays following fields:

Field	Action/Description
Certificate ACL Name	Name or Tag associated with the Certificate Map.
Certificate ACL Entries and Criteria	
Certificate ACL Entry	To add a new ACL Entry, enter the ACL sequence number in the New ACL Entry field, then click >> Add . To remove an ACL Entry, select the ACL entry from the sequence list, then click << Remove .
Sequence	The sequence number of the ACL entry. Valid range is from 1 to 65535.
Certificate Field	Select one of the following certificate field to be examined for Access Control: <ul style="list-style-type: none"> • Subject Name • Alternate Subject Name • Any subject name field • Unstructured subject name • Issuer name • Valid start date • Expiry date

Field	Action/Description
Match Condition	The following match conditions are supported: <ul style="list-style-type: none"> • Equals (eq) • Not Equals (neq) • Contains (co) • Not Contains (nco) • Less than (lt) • Greater than or Equals (ge)
Match Value	Certificate Field value

To add new criteria to the ACL entry, select a certificate field and match condition, then enter the match value and click **Add**. The values you entered appears in the table. To remove a criteria from the ACL entry, select a row in the table, then click **Remove**.

Step 3 Click **OK** to complete the task.

Editing Certificate ACLs

Step 1 Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Certificate ACLs** from the object selector. The Certificate ACLs page appears.

Step 2 Select a Certificate ACL from the list, then click **Edit**. The Edit Certificate Map dialog box appears.

Using this dialog box you can:

- Add a new ACL entry
- Remove an existing ACL entry
- Add new criteria to an existing ACL entry
- Remove criteria from an existing ACL entry.

The page displays following fields:

Field	Description
Certificate ACL Name	Name associated to the Certificate ACL
Certificate ACL Entries and Criteria	
Certificate ACL Entry	To add a new ACL Entry, enter the ACL sequence number in the New ACL Entry field, then click ADD . To remove an ACL Entry, select the ACL entry from the sequence list, then click Remove .
Sequence	The sequence number of the ACL entry. Valid range is from 1 to 65535.
Certificate Field	Select one of the following certificate field to be examined for Access Control: <ul style="list-style-type: none"> • Subject Name • Alternate Subject Name • Any subject name field • Unstructured subject name • Issuer name • Valid start date • Expiry date

Field	Description
Match Condition	The following match conditions are supported: <ul style="list-style-type: none"> • Equals (eq) • Not Equals (neq) • Contains (co) • Not Contains (nco) • Less than (lt) • Greater than or Equals (ge)
Match Value	Certificate Field value

To add new criteria to the ACL entry, select a certificate field and match condition, then enter the match value and click **Add**. The values you entered appears in the table. To remove a criteria from the ACL entry, select a row in the table, then click **Remove**.

Step 3 Click **OK** to add the certificate ACL.

Deleting Certificate ACLs

Step 1 Click **Setup** at the top of the window, click **PKI** in the left-most pane, and select **Trustpoints > Certificate ACLs** from the object selector. The Certificate ACLs page appears.

Step 2 Select a certificate ACL, then click **Delete**.

•

■ Deleting Certificate ACLs



Managing Proxy Services

CVDM-SSLSM allows you to view, configure, and edit Proxy Services. The Proxy Service Wizards helps you set up proxy services.

This chapter contains the following topics:

- [Proxy Service Wizards, page 7-2](#)
- [Viewing Proxy Services, page 7-15](#)
- [Viewing Proxy Services Details, page 7-18](#)
- [Troubleshooting Proxy Services, page 7-33](#)
- [NAT Pools, page 7-26](#)

You can configure the virtual IP address and port associated with the proxy service, and the associated target server IP address and port. You can define TCP and SSL policies for both client (virtual) and server sides of the proxy.

You can configure SSL client proxy services to specify that the proxy service accepts clear text traffic, encrypts the traffic into SSL traffic, and forwards the traffic to the backend SSL server.

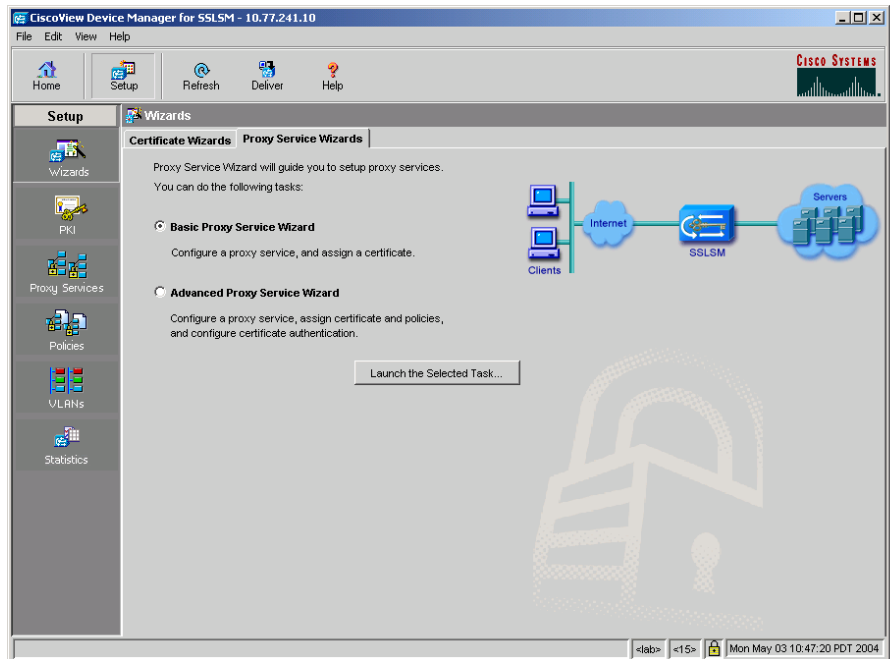
While you are required to configure a certificate for the SSL server proxy, you are not required to configure a certificate for SSL client proxy. If you configure the certificate for the SSL client proxy, that certificate is sent in response to the Certificate Request message that is sent by the server during the client authentication phase of the handshake protocol.

Proxy Service Wizards

CVDM-SSLSM supports the following proxy service wizards. You can use the basic Proxy Service Wizard to configure a proxy service and assign a certificate. The advanced proxy service wizards helps you to configure the proxy service, assign a certificate and policies, and configure peer certificate authentication.

- [Basic Proxy Service Wizard, page 7-3](#)
- [Advanced Proxy Service Wizard, page 7-8](#)

Figure 7-1 Proxy Service Wizards



113573

Basic Proxy Service Wizard

The Basic Proxy Service wizard helps you set up a server proxy service or a client proxy/backend encryption service.

To launch the basic proxy service wizard:

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **Wizards** in the left-most pane. The Wizards page appears.
 - Step 3** Click **Proxy Services Wizard** tab. The Proxy services wizard page appears.
 - Step 4** Select **Basic Proxy Service Configuration**, then click **Launch the Selected Task**. The Welcome page for basic proxy service wizard appears.
 - Step 5** The Welcome page describes the steps to follow for creating a proxy service. Click **Next** to continue.
-

To create a proxy service:

-
- Step 1** Define the proxy service name and type. For more information on defining the name and type, see [Defining Proxy Service Name and Type, page 7-4](#).
 - Step 2** Configure the client side (virtual) parameters and server parameters. For more information on configuring the client side (virtual) parameters and the server parameters, see [Configuring Client Side \(Virtual\) and Server Parameters, page 7-5](#).
 - Step 3** Assign certificate to proxy service (optional for client proxy service). For more information on assigning certificates to a proxy service, see [Assigning Certificate to Proxy Services, page 7-6](#).
-

Defining Proxy Service Name and Type

This page of the basic proxy service setup wizard helps you define the name and type of the proxy service.

The following fields appear:

Field	Description
Proxy Service Name	Enter a name for your proxy service.
Admin Status	Select the admin status of the proxy service. Values are: <ul style="list-style-type: none"> • Up • Down
Service Type	
Server Proxy	Select this option if you want to create a server proxy service. Server proxy service accepts clear text traffic, encrypts the traffic into SSL traffic, and forwards it to the backend SSL Server.
Client Proxy / Backend Encryption	Select this option if you want to create a client proxy service. Client server proxy service accepts SSL traffic, decrypts the traffic into clear text, and forwards it to the backend server or virtual server.

Click < **Back** to read the welcome page.

Click **Next** > to move to step 2 of the task.

Configuring Client Side (Virtual) and Server Parameters

This page of the basic proxy setup wizard helps you in configuring the client side parameters and server parameters. You can configure NAT and also enable SSL Version 2.0 connections to be forwarded to a server using this page.

The following fields appear:

Field	Description
Client Side (Virtual)	
Virtual IP Address	Enter the virtual IP address.
Secondary	Select the checkbox if you want to use the IP address as a secondary IP address.
Virtual IP Mask	Select any one of the following netmasks: <ul style="list-style-type: none"> • 0.0.0.0 • 255.0.0.0 • 255.255.0.0 • 255.255.255.0
Wildcard Virtual IP Address	Select the checkbox to configure a wildcard virtual IP address.
Port (1-65535)	Enter the number of the port to be used for proxy service traffic.
Server	
Server IP Address	Enter the server IP address.
Port (1-65535)	Enter the number of the port to be used for the traffic.
NAT	
Server NAT	Select the check-box if you want to use a Server NAT.
Client NAT	Select the check-box if you want to use a Server NAT.
Client NAT Pool	Select any of the following options: <ul style="list-style-type: none"> • Create and assign a new NAT Pool. • Select an existing NAT Pool. • Clear the NAT pool.

Field	Description
Forward SSL version 2.0 Connections	Select the check-box if you want to forward SSL version 2.0 connection to a SSLv2 server.
Server IP Address	The IP address of the server to be used for SSL version 2.0.
Port (1-65535)	The port to be used for the traffic.

Click < **Back** to move back to Step 1 of the basic setup wizard.

Click **Next** > to move to step 3 of the basic setup wizard.

Assigning Certificate to Proxy Services

This page of the Basic Proxy Service setup wizard helps you assign a certificate to the proxy service.

The following fields are displayed:

Field	Description
Certificate	
Certificate Trustpoint	Select one of the following options: <ul style="list-style-type: none"> Select an existing Trustpoint. Clear the Trustpoint.
Status	Displays the status of the certificate.

Selecting Available Certificate Trustpoints

The available certificate Trustpoints dialog box provides information on the certificate Trustpoints available for the proxy services.

The following fields appear:

Field	Description
Trustpoint	The name of the Trustpoint.
Certificate Authority (CA)	The certification authority details of the certificate Trustpoint.
Subject	The subject of the certificate Trustpoint.

Select a Trustpoint, then click **OK** to select an existing certificate Trustpoint.

Viewing Proxy Service Setup Summary

From this window you can view a summary of the configured settings. You can review the configuration information.

Click **< Back** to move to the previous page of the wizard.

Click **Finish** to complete the setting up of proxy service.

Advanced Proxy Service Wizard

The Advanced Proxy Service wizard helps you in setting up a server proxy service or a client proxy/backend encryption service, and allows you to configure certificate authentication. The wizards also helps you set up policies for client (virtual) side and server connections.

To launch the advanced proxy service wizard:

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **Wizards** in the left-most pane. The Wizards page appears.
 - Step 3** Click **Proxy Services Wizard** tab. The Proxy services wizard page appears.
 - Step 4** Select **Advanced Proxy Service Configuration**, then click **Launch the Selected Task**. The Welcome page of the basic proxy service wizard appears.
 - Step 5** The Welcome page describes the steps to follow for creating a proxy service. Click **Next** to continue.
-

To create a proxy service:

-
- Step 1** Define Proxy Service Name and Type.
 - Step 2** Configure Client Side (Virtual) and Server Parameters.
 - Step 3** (Optional for client proxy service) Assign Certificate to Proxy Service.
 - Step 4** (Optional) Assign policies to proxy service.
-

Defining Proxy Service Name and Type

This page of the Advanced Proxy Service setup wizard helps you in defining proxy service name and type.


The following fields appear:

Field	Description
Proxy Service Name	Enter a name for your proxy service.
Admin Status	Select the admin status of the proxy service. Values are: <ul style="list-style-type: none">• Up• Down
Service Type	
Server Proxy	Select this option if you want to create a server proxy service. Server proxy service accepts clear text traffic, encrypts the traffic into SSL traffic, and forwards it to the backend SSL Server.
Client Proxy / Backend Encryption	Select this if option if you want to create a Client proxy service. Client server proxy service accepts SSL traffic, decrypts the traffic into clear text, and forwards it to the backend server or virtual server.

Configuring Client Side (Virtual) and Server Parameters

This page of the advanced proxy setup wizard helps you in configuring the client side parameters and server parameters. You can configure NAT using this page and also enable SSL Version 2.0 connections to be forwarded to a server.

The following fields appear:

Field	Description
Client Side (Virtual)	
Virtual IP Address	Enter the virtual IP address.
Secondary	Select the check-box if you want to make the sever secondary.
Virtual Netmask	Select any one of the following netmasks: <ul style="list-style-type: none"> • 0.0.0.0 • 255.0.0.0 • 255.255.0.0 • 255.255.255.0
Wildcard Virtual IP Address	Select this checkbox to configure a wildcard virtual IP address.
Port (1-65535)	Enter the number of the port to be used for proxy service traffic.
Server	
Server IP Address	Enter the server IP address.
Port (1-65535)	Enter the number of the port to be used for the traffic.
NAT	
Server NAT	Select the checkbox if you want to use a server NAT.
Client NAT Pool	Click  and select any of the following options: <ul style="list-style-type: none"> • Create and assign a new NAT Pool. • Select an existing NAT Pool. • Clear the NAT pool.


Click < **Back** to move back to Step 1 of the basic setup wizard.

Click **Next** > to move to step 3 of the basic setup wizard.

Assigning Certificate to Proxy Service

This page of the advanced proxy setup wizard helps you in assigning a certificate to the proxy service.

The following fields appear:

Field	Description
Certificate	
Certificate Trustpoint	Click  and select one of the following options: <ul style="list-style-type: none"> Select an existing Trustpoint. Clear the Trustpoint.
Status	Displays the status of the certificate.
Peer Certificate Authentication	
Certificate Authentication	Enable or disable the certificate authentication.
Trusted CA Pool	The name of the trusted CA Pool.

Assigning Policies to Proxy Services

This page of the wizard helps you to assign policies to virtual and server proxy services.

The following fields appear:

Field	Description
Client Side (Virtual) TCP Policy	Select a client side TCP policy.
Client Side (Virtual) SSL Policy	Select a client side SSL policy.
Server TCP Policy	Select a server TCP policy.

Field	Description
Server SSL Policy	Select a server SSL policy.
URL Rewrite Policy	Select a URL rewrite policy.
HTTP Header Insertion Policy	Select an HTTP header insertion policy.

The dialog box helps you to:

- Create and use a new policy.
- Select an existing policy. You can select a policy from the list of existing policies.
- Clear the policy.

Assigning TCP Policy to Proxy Services

This page of the wizard helps you to assign policies to virtual and server proxy services.

The following fields appear:

Field	Action/Description
Policy	The name of the TCP Policy.
Proxy Service Name	The name of the proxy service.
Client Side (Virtual)	The name of the client side server.
Selected Services	The list of selected services.
Side	Select one of the following: Both-the policy is assigned to both server and client. Client-the policy is assigned to client only. Server-the policy is assigned to server only.

To assign a policy:

-
- Step 1** Select a proxy service name from the table, then click **Add>>**. The proxy service name is added to the list of selected services.
 - Step 2** Select the side to which the policy has to be assigned.
 - Step 3** Click **OK**.
-

Viewing Advanced Proxy Service Setup Summary

The summary page of the Advanced Proxy Service setup wizard provides the details of the proxy service you have configured.

Click **< Back** to move to step 3 of the wizard.

Click **Finish** to complete the setting up of proxy service.

Selecting Available NAT Pools

The Available NAT Pools dialog box provides information on the NAT Pools configured on the SSLSM.

Select a NAT Pool from the list, then click **OK** to select a NAT Pool.

The following fields appear:

Field	Description
Name	Name of the NAT pool.
Start IP Address	The first IP address in the NAT pool.
End IP Address	The last IP address in the NAT pool.
Netmask	The Netmask used by the addresses in the NAT pool.

Selecting Available CA Pools

The Available CA Pools dialog box provides information on the CA Pools configured on the SSLSM.

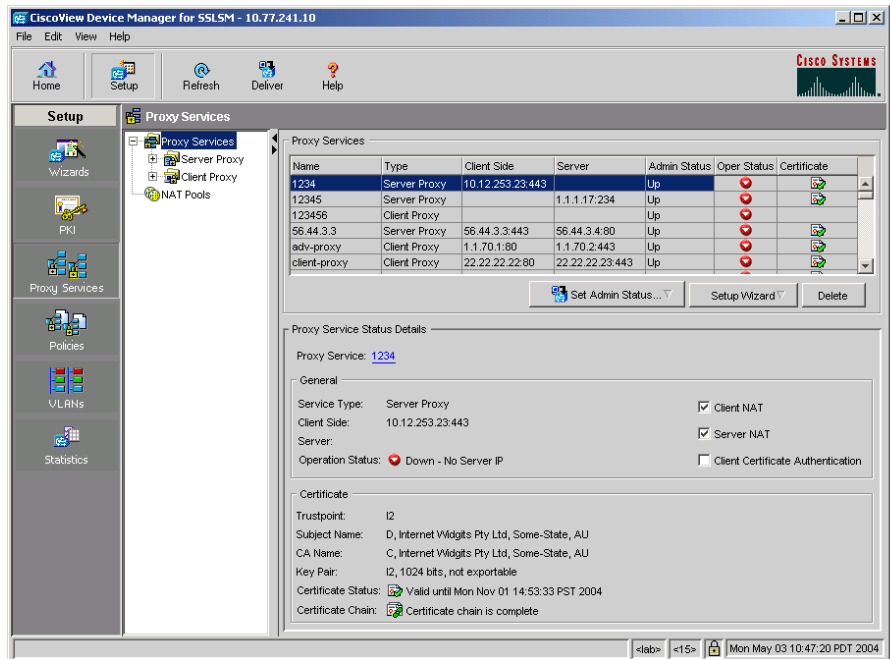
Select a CA Pool from the list, then click **OK** to select a CA Pool.

The following fields appear:

Field	Description
Name	The name of the CA Pool.
Number of Trustpoints	The number of Trustpoints associated to each CA Pool.
Status	The status of the CA Pool.

Viewing Proxy Services

Figure 7-2 Proxy Services













To view proxy services:

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Proxy Services**. The proxy services page appears.
- Step 3** Open Proxy Services Group Folder. Proxy services are grouped under two sub-group folders:
 - Server Proxy Services
 - Client Proxy Services

Step 4 Click any of the sub-group folder.

The following fields appear:

Field	Description
Proxy Services	
Name	Name of the proxy service.
Type	The type of the proxy service.
Client Side	The IP address and port number of the client.
Server	The IP address and port number of the server.
Admin Status	The admin status of the service.
Oper Status	Indicates the operational status of the service. A  icon indicates that the service is administratively down. A  icon indicates that the service is operationally down. A  icon indicates that the service is up.
Certificate	Indicates the status of the certificate. A  icon indicates that the certificate is valid. A  icon indicates that the certificate is invalid. A  icon indicates that the certificate is valid only for less than 10 days. A  icon indicates that the certificate is valid only for less than 20 days. A  icon indicates that the certificate is valid only for less than 30 days. A  icon indicates that the certificate chain is complete. A  icon indicates that the certificate chain is incomplete.

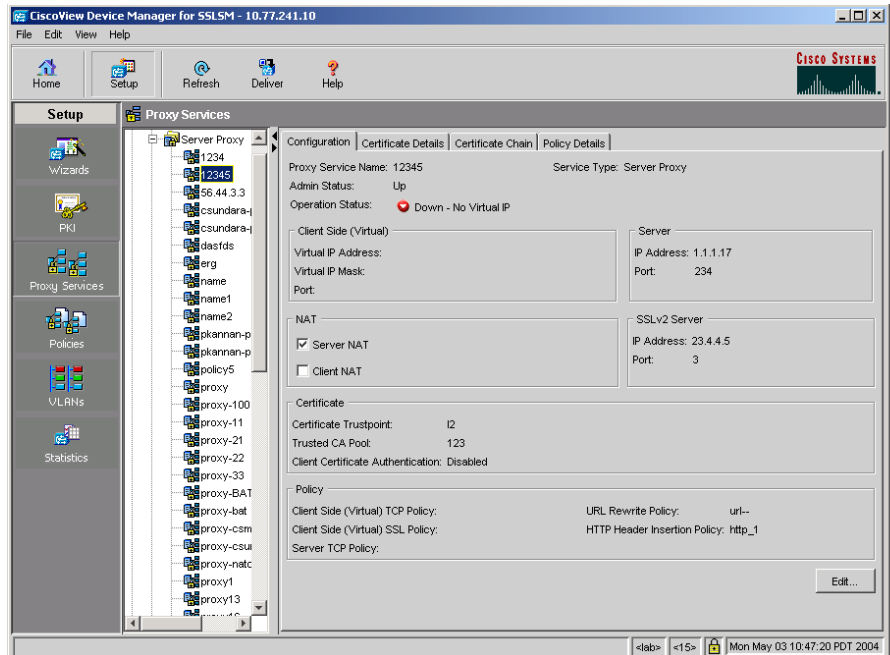
Select any of the proxy service from the table, the following information appears for the selected service:

Proxy Service Status Details

Field	Description
Proxy Service	Name of the proxy service.
General	
Service Type	The type of the service provided by the proxy. For example: Server Proxy
Client Side	The IP address and port number of the client.
Server	The IP address and port number of the server.
Operation Status	Indicates the operational status of the service.
Client NAT	Indicates whether the client NAT is enabled.
Server NAT	Indicates whether the server NAT is enabled.
Server/Client Certificate Authentication	Indicates whether the peer certificate authentication is enabled.
Certificate	
Trustpoint	Name of the certificate Trustpoint associated with the proxy service.
Subject Name	The subject name of the associated certificate.
CA Name	The issuer name of the associated certificate.
Key Pair	The key pair name, key size and indicates whether key pair is exportable.
Certificate Status	Indicates the validity of the certificate.
Certificate Chain	Indicates the status of the certificate chain.

Viewing Proxy Services Details

Figure 7-3 Proxy Service Details



113572

To view the configured proxy services:

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Proxy Services**. The proxy services page appears.
- Step 3** Open Proxy Services Group Folder. Proxy services are grouped under two sub-group folders:
 - Server Proxy
 - Client Proxy
- Step 4** Open any of the sub-group folder, then click any of the object in the sub-group folder.

You can also view the details by clicking the proxy service hyperlink in the proxy service status details panel

The following fields appear:

Field	Description
Configuration	
Proxy Service Name	Name of the proxy service
Admin Status	The administrative status of the proxy service.
Service Type	The type of the proxy service handled by the proxy service.
Operation Status	The operation status of the proxy service.
Client Side (Virtual)	
Virtual IP Address	The client side IP address of the proxy service.
Virtual IP Mask	The client side mask used by the proxy service.
Port	The TCP port used by the client side proxy service.
Server	
IP Address	The server IP address used by the proxy service.
Port	The TCP port used by the server side proxy service.
NAT	
Server NAT	Indicates whether the server NAT is enabled.
Client NAT	Indicates whether the client NAT is enabled.
Client NAT Pool	The client NAT Pool used by the proxy service.
SSLV2 Server	
IP Address	The IP address of the SSLV2 server used by the service.
Port	The port used by the SSLv2 server.
Certificate	
Certificate Trustpoint	The name of the certificate Trustpoint associated by the service.
Trusted CA Pool	The name of the trusted CA pool used by the service.

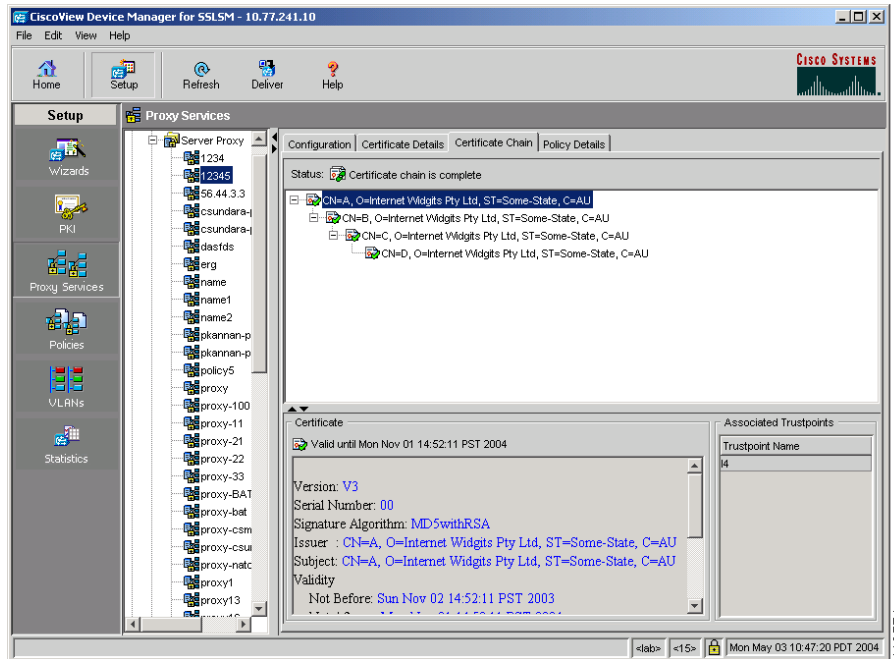
Field	Description
Server/Client Certificate Authentication	Indicates whether a peer certificate authentication is being used.
Policy	
Client Side (Virtual) TCP Policy	The virtual TCP policy used by the service.
Client Side (Virtual) SSL Policy	The virtual SSL policy used by the service.
Server TCP Policy	The server TCP Policy used by the service.
URL Rewrite Policy	The URL rewrite policy used by the service.
HTTP Header Insertion Policy	The HTTP header insertion policy used by the service.

Click **Certificate Details** Tab to view the Certificate details.

Field	Description
Certificate Status	The status of the certificate used by the selected service. Example: Valid until Tue Nov 02 04:22:11 GMT +05:30 2004
Trusted CA Certificates	
CA Name	The name of the CA associated with the service.
Certificate Status	The status of the certificate.
Associated Trustpoint	Trustpoints associated with the certificate.

Click **Certificate Chain** Tab to view the Certificate chain.

Figure 7-4 Proxy Service - Certificate Chain



Field	Description
Status	The status of the certificate chain. Example: Certificate chain is complete.
Certificate	Displays the time until which the certificate is valid and the certificate. Example: Valid until Tue Nov 02 04:22:11 GMT +05:30 2004
Associated Trustpoints	This field appears only if the certificate has an associated Trustpoint.

Click **Policy Details** Tab to view the Certificate chain.

Field	Description
Policies	<p>The list of applicable policies.</p> <ul style="list-style-type: none"> • Client Side (Virtual) SSL policy • Client Side (Virtual) TCP policy • Server TCP Policy • URL Rewrite Policy • HTTP Header Insertion policy <p>Select any of the policies to view the details.</p>
Policy Details	The content in the policy details area changes according to the policies you select.

Editing Proxy Service Configuration

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Proxy Services**. The proxy services page appears.
- Step 3** Open Proxy Services Group Folder. Proxy services are grouped under two sub-group folders:
- Server Proxy Services
 - Client Proxy Services
- Step 4** Open any of the sub-group folder, then click any of the object in the sub-group folder. The proxy service details page appears.
- Step 5** Click **Edit...**
- The following information appears:

Field	Action/Description
Proxy Service Name	Name of the proxy service you are editing.
Admin Status	Select the admin status for the service.

Field	Action/Description
Client Side (Virtual)	
Virtual IP Address	Enter the virtual IP address for the service.
Secondary	Select the checkbox if you need to make the virtual IP address a secondary IP address. Secondary is required if the IP address is not on a directly connected network.
Virtual IP Mask	Select wildcard virtual IP address option to make this field active. Select the IP mask from the drop-down list.
Wildcard Virtual IP Address	Select this option to use wildcard IP address.
Port (1-65535)	Enter the port number to be used by the service.
Server	
IP Address	Enter the server IP address.
Port (1-65535)	Enter the port number used by the server.
SSLV2 Server	
IP Address	Enter the IP address of the SSLV2 server.
Port (1-65535)	Enter the port number to be used by the server.
NAT	
Server NAT	Select this option to use a server NAT.
Client NAT	Select this option to use a server NAT.
Client NAT Pool	Select one of the following: <ul style="list-style-type: none"> • Create and use a new NAT Pool • Select an existing NAT Pool • Clear the NAT Pool

To edit the certificate details of the service, click Certificate tab. The following fields appear:

Field	Action/Description
Certificate Trustpoint	Select any of the following options: <ul style="list-style-type: none"> • Select an existing Trustpoint • Clear the Trustpoint
Trusted CA Pool	Select any of the following options: <ul style="list-style-type: none"> • Create and use a new CA Pool • Select an existing CA Pool • Clear the CA Pool
Client/Server Certificate Authentication	Select any of the following options: <ul style="list-style-type: none"> • Disabled • Verify Signature, Check CRL and Certificate ACL • Verify Signature Only

To edit the policy details of the service, click Policy tab. The following fields appear:

Field	Action/Description
Client Side (Virtual) TCP Policy	Select any of the following: <ul style="list-style-type: none"> • Create and use a new TCP Policy • Select an existing TCP Policy • Clear TCP Policy
Client Side (Virtual) SSL Policy	Select any of the following: <ul style="list-style-type: none"> • Create and use a new SSL Policy • Select an existing SSL Policy • Clear SSL Policy

Field	Action/Description
Server TCP Policy	Select any of the following: <ul style="list-style-type: none">• Create and use a new TCP Policy• Select an existing TCP Policy• Clear TCP Policy
Server SSL Policy	Select any of the following: <ul style="list-style-type: none">• Create and use a new SSL Policy• Select an existing SSL Policy• Clear SSL Policy
URL Rewrite Policy	Select any of the following: <ul style="list-style-type: none">• Create and use a new URL Rewrite Policy• Select an existing URL Rewrite Policy• Clear URL Rewrite Policy
HTTP Header Insertion Policy	Select any of the following: <ul style="list-style-type: none">• Create and use a new HTTP Header Insertion Policy• Select an existing HTTP Header Insertion Policy• Clear HTTP Header Insertion Policy

NAT Pools

CVDM-SSLSM allows you to create Network Address Translation (NAT) pools.

Figure 7-5 NAT Pools

Name	Start IP Address	End IP Address	Netmask	Use Count
1.1.70.1	1.1.70.3	1.1.70.10	255.0.0.0	0
csundara-2	10.77.1.10	10.77.1.17	255.255.255.0	0
csundara-pool-3	10.1.253.12	10.1.253.19	255.255.255.0	0
nat-1	11.2.254.61	11.2.254.68	255.255.255.0	1
nat-2	11.2.253.41	11.2.253.48	255.255.255.0	0
nat-60	11.2.253.61	11.2.253.68	255.255.255.0	1
nat-90	11.2.253.91	11.2.253.98	255.255.255.0	1
nat1	1.1.1.3	1.1.1.10	255.0.0.0	1
nat11	12.12.14.3	12.12.14.10	255.0.0.0	1
nat13	12.12.14.31	12.12.14.38	255.0.0.0	0
nat16	1.1.16.3	1.1.16.10	255.0.0.0	1
nat17	1.1.17.1	1.1.17.8	255.0.0.0	1
nat18	1.1.18.8	1.1.18.15	255.0.0.0	1
nat19	1.1.19.3	1.1.19.10	255.255.0.0	0
nat24	1.1.24.3	1.1.24.10	255.0.0.0	1

NAT Pool Details: 1.1.70.1		
General		
Start IP Address:	1.1.70.3	
End IP Address:	1.1.70.10	
Netmask:	255.0.0.0	
Associated VLAN:	No matching VLAN	
Use Count:	0	
Associated Proxy Services		
Name	Client Side	Server

This section describes the following topics:

- [Viewing NAT Pools, page 7-28](#)
- [Adding NAT Pools, page 7-29](#)
- [Deleting NAT Pools, page 7-30](#)
- [Assigning NAT Pools to Proxy Services, page 7-30](#)

Understanding NAT Pools

Client connections originate from the client and are terminated on the SSL Services Module. Server connections originate from the SSL Services Module. You can configure client NAT, server NAT, or both, on the server connection.

Server NAT

If you configure server NAT, the server IP address is used as the destination IP address for the server connection. If the server NAT is not configured, the destination IP address for the server connection is the same as the virtual IP address for which SSL Services Module is a proxy.

Client NAT

If you configure client NAT, the server connection source IP address and port are derived from a NAT pool. If client NAT is not configured, the server connection source IP address and port are derived from the source IP address and source port of the client connection.

Allocate enough IP addresses to satisfy the total number of connections supported by the SSL Services Module (256,000 connections). Assuming you have 32,000 ports per IP address, configure 8 IP addresses in the NAT pool. If you try to configure fewer IP addresses than required by the total connections supported by the SSL Services Module, the command is rejected.

Viewing NAT Pools

- Step 1** Click **Setup** in the task bar.
- Step 2** Click **Proxy Services** in the left-most pane. The Proxy Services page appears.
- Step 3** Click **NAT Pools** in the object selector.

The following information appears:

Field	Description
Name	The Name of the NAT Pool.
Start IP Address	The first IP address used by the NAT Pool.
End IP Address	The last IP address used by the NAT Pool.
Netmask	The netmask used for the NAT pool. For example: 255.255.0.0
Use Count	Number of proxy services using the NAT pool.

Select a NAT Pool, then click **Assign to Proxy Services** to assign a NAT Pool to a proxy service

Click **Add...** to add a new NAT Pool.

Select a NAT Pool, then click **Delete** to delete a NAT Pool.

- Step 4** Select any NAT Pool from the table to display the configuration details.

Field	Description
General	
Start IP Address	The first IP address in the NAT pool.
End IP Address	The last IP address in the NAT pool.
Netmask	The netmask used for the NAT pool. For example: 255.255.255.0
Associated VLAN	The VLAN associated with the NAT pool.
Use Count	The number of proxy services associated with the NAT Pool.
Associated Proxy Services	
Name	The name of the associated proxy service.
Client Side	The IP address of the virtual server.
Server	The IP address of the server.

Adding NAT Pools

- Step 1** Click **Setup** in the task bar.
- Step 2** Click **Proxy Services** in the left-most pane. The Proxy Services page appears.
- Step 3** Click **NAT Pools** in the object selector.
- Step 4** Click **Add...** The Add New NAT Pool dialog box appears.

Field	Description
NAT Pool Name	Enter a name for your new NAT Pool.
Start IP Address	Enter the first IP address to be used for the NAT Pool.
End IP Address	Enter the last IP address to be used for the NAT Pool.
Net Mask	The IP mask to be used by the NAT Pool.

Alternatively, you can add NAT Pools using the Wizards.

Deleting NAT Pools

- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **Proxy Services** in the left-most pane. The Proxy Services page appears.
 - Step 3** Click **NAT Pools** in the object selector.
 - Step 4** Select a NAT pool from the list, then click **Delete**.
-

Assigning NAT Pools to Proxy Services

- Step 1** Click **Setup** in the task bar.
- Step 2** Click **Proxy Services** in the left-most pane. The Proxy Services page appears.
- Step 3** Click **NAT Pools** in the object selector.
- Step 4** Select a NAT pool from the list, then click **Assign to Proxy Services**. The Assign NAT Pool to Proxy Services dialog box appears.

Field	Description
Pool Name	The name of the NAT Pool you have selected.
Proxy Service Name	The name of the proxy service. You can select any one of the service from the list.
Client Side (Virtual)	Virtual server associated with the proxy service.
Selected Proxy Services	The list of services to which you want to assign the NAT Pool.

- Step 5** Select a Proxy Service Name, then click **Add >>** to add the policy to the selected service.

You can remove the a proxy service from the list. Select a service from the list, then click << **Remove**.

You can clear all the services selected for assigning to a policy. Select a service from the list, then click **Clear All**.

Step 6 Click **OK** to assign NAT pool to the selected proxy services.

Selecting Available CA Pools

The following information appears:

Field	Action/Description
Name	Name of the CA Pool.
Number of Trustpoints	Number of Trustpoints associated with the CA Pool.
Status	Indicates the status of the CA Pool.

Select a CA Pool from the table, then click **OK**.

Selecting Available NAT Pools

The following information appears:

Field	Action/Description
Pool Name	Name of the NAT pool.
Start IP Address	The start IP address of the pool.
End IP Address	The end IP address of the pool.
Netmask	The netmask and port used by the selected NAT pool.

Select a NAT Pool from the table, then click **OK**.

Selecting Available Certificate Trustpoints

The following information appears:

Field	Action/Description
Trustpoint	The name of the Trustpoint.
Certificate Authority (CA)	The certificate authority details in the certificate.
Subject	The subject in the certificate.

Select a Certificate Trustpoint from the table, then click **OK**.

How Do I...

This section describes on how to achieve a task. The following question is answered:

- [How Do I Setup a Proxy Service?](#)

How Do I Setup a Proxy Service?

You can use Proxy Service Setup Wizards to create a proxy service.

The Basic Proxy Service wizard helps you set up a server proxy service or a client proxy/backend encryption service.

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **Wizards** in the left-most pane. The Wizards page appears.
 - Step 3** Click **Proxy Services Wizard** tab. The Proxy services wizard page appears.
 - Step 4** Select **Basic Proxy Service Configuration**, then click **Launch the Selected Task**. The Welcome page for basic proxy service wizard appears. The Welcome page describes the steps to follow to complete the task.
 - Step 5** Click **Next** to continue.

- Step 6** Define the proxy service name and type. For more information on defining the name and type, see [Defining Proxy Service Name and Type, page 7-4](#)
- Step 7** Click **Next** to continue.
- Step 8** Configure the client side (virtual) parameters and server parameters. For more information on configuring the client side (virtual) parameters and the server parameters, see [Configuring Client Side \(Virtual\) and Server Parameters, page 7-5](#).
- Step 9** Click **Next** to Continue.
- Step 10** Assign certificate to proxy service (optional for client proxy service). For more information on assigning certificates to a proxy service, see [Assigning Certificate to Proxy Services, page 7-6](#).

Troubleshooting Proxy Services

This section describes the proxy service operations status and the possible cause.

Proxy Service Operation Status	Possible Cause/Action
No cert	The certificate Trustpoint associated with the proxy service does not have a valid certificate or the certificate chain is incomplete. You must make sure that the Trustpoint has a valid certificate and that the certificate chain is complete.
No Virtual IP	Virtual IP address has not been configured for the proxy service.
No Server IP	Server IP address has not been configured for the proxy service.

Proxy Service Operation Status	Possible Cause/Action
Cert not configured	No certificate has been configured for the proxy service. You must assign a certificate for server proxy service. For client proxy service a certificate is optional.
No CA pool	If you have enabled peer certificate authentication to verify all (signature, CRL check and ACL check), you must configure a CA pool with valid CA certificates for the proxy service.

Proxy Service Operation Status	Possible Cause/Action
No connectivity	<p data-bbox="799 238 1002 266">No Client VLAN</p> <p data-bbox="799 285 1210 375">If the virtual IP address (VIP) is not secondary, you must configure a VLAN for the client side network.</p> <p data-bbox="799 394 1233 516">If you configure the VIP as secondary, it does not have to be in the VLAN (subnet) connected to the SSL Services Module.</p> <p data-bbox="799 535 1009 563">No Server VLAN</p> <p data-bbox="799 583 1224 704">If the server is in a network that is directly connected to SSL Services Module, you must configure a VLAN for the server side network.</p> <p data-bbox="799 724 1150 813">If the server is not in a directly connected network, you must configure a route to the server.</p> <p data-bbox="799 833 1092 860">No SSLv2 Server VLAN</p> <p data-bbox="799 880 1224 1060">If you have enabled forwarding of SSLv2 connections to a server and if the SSLv2 server is in a directly connected network, you must configure a VLAN for the server side network.</p> <p data-bbox="799 1079 1233 1169">If the SSLv2 server is not in a directly connected network, you must configure a route the SSLv2 server.</p> <p data-bbox="799 1188 1116 1216">No Server/Next Hop MAC</p> <p data-bbox="799 1235 1233 1292">The server or the next hop (gateway) to the server is not responding to ARP.</p> <p data-bbox="799 1312 1201 1339">No SSLv2 Server/Next Hop MAC</p> <p data-bbox="799 1359 1214 1448">The SSLv2 server or the next hop (gateway) to the SSLv2 server is not responding to ARP.</p>



Managing Policies

The CVDM-SSLSM supports defining policies for Proxy Services. The policy templates help the Administrator customize the attributes associated with SSL and TCP stack to suit the needs.

The following policies are supported by the SSLSM:

- [SSL Policy, page 8-10](#)
- [TCP Policy, page 8-3](#)
- [HTTP Header Insertion Policy, page 8-17](#)
- [URL Rewrite Policy, page 8-23](#)

Policies are grouped by their type and are displayed as a tree node in the object selector. All configured policies of a type are listed as child nodes under the policy node.

Figure 8-1 Policies Page

The screenshot shows the CiscoView Device Manager for SSLSM interface. The main window displays the Policies page, which includes a table of SSL Policies and a detailed view for the selected policy.

SSL Policies Table:

Policy Name	Number of Proxy Services Assigned
ssl_1	2
ssl_2	0
ssl3	1
ssl4	0
ssl--	1
ssl6	0
ssl7	0
ssl_3	0
nagopal2	0
nagopal3	0
nagopa1	0
nagopa5	0

SSL Policy Details for ssl_1:

Policy Name: ssl_1

Version: TLS1

Close Protocol: Disabled

Session Cache: Enabled

Handshake Timeout (Secs):

Session Timeout (Secs):

Session Cache Size:

Acceptable Cipher-Suites:

Cipher Suites:

- rsa-with-rca4-128-md5
- rsa-with-rca4-128-sha
- rsa-with-des-cbc-sha
- rsa-with-3des-ede-cbc-sha

113570

TCP Policy

The TCP commands for the SSL Services Module apply either globally or to a particular proxy server.

The TCP policy template allows you to define parameters associated with the TCP stack.

Viewing TCP Policies

To view the TCP Policies:

-
- Step 1** Click **Setup** from the task bar.
 - Step 2** Click **Policies** from the left-most pane, then select **TCP Policy** from the object selector. The policy information appears on the page.

The following fields appear:

TCP Policies

Fields	Description
Policy Name	Name of the TCP Policy
Number of Proxy Services (Use Count)	Number of proxy services using the TCP Policy.

Select a policy, then click **Assign to Proxy Services** to assign a policy to the proxy services.

Click **Add** to add a new TCP policy. The Add TCP Policy dialog box appears.

Select a policy, then click **Edit** to edit a TCP policy. The Edit TCP Policy dialog box appears.

Select a policy, then click **Delete** to delete the policy.

- Step 3** Select a policy from the TCP Policy table, then click **Policy Tab** to view the policy details or click **Associated Proxy Services** tab to view the proxy services associated with the policies.

TCP Policy Details

Fields	Description
Policy	
Policy Name	Name of the TCP Policy.
MSS	The maximum segment size (MSS), in bytes, that the connection will identify in the SYN packet that it generates.
Syn Timeout	The connection establishment timeout.
Inactivity Timeout	The amount of time, in seconds, that an established connection can be inactive.
Reassembly Timeout	The amount of time, in seconds, before the reassembly queue is cleared. If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped.
Fin Timeout	The FIN wait timeout in seconds.
Buffer Share Rx	The maximum receive buffer share per connection in bytes.
Buffer Share Tx	The maximum transmit buffer share per connection in bytes.
Associated Proxy Services	
Name	The name of the associated proxy service.
Type	Type of the proxy service.
Side	Indicates whether the policy is applied to the client side or server side of the proxy service.
Virtual Server	The IP address of the virtual server.
Server	The IP address of the server.
Oper Status	The operational status of the proxy server.

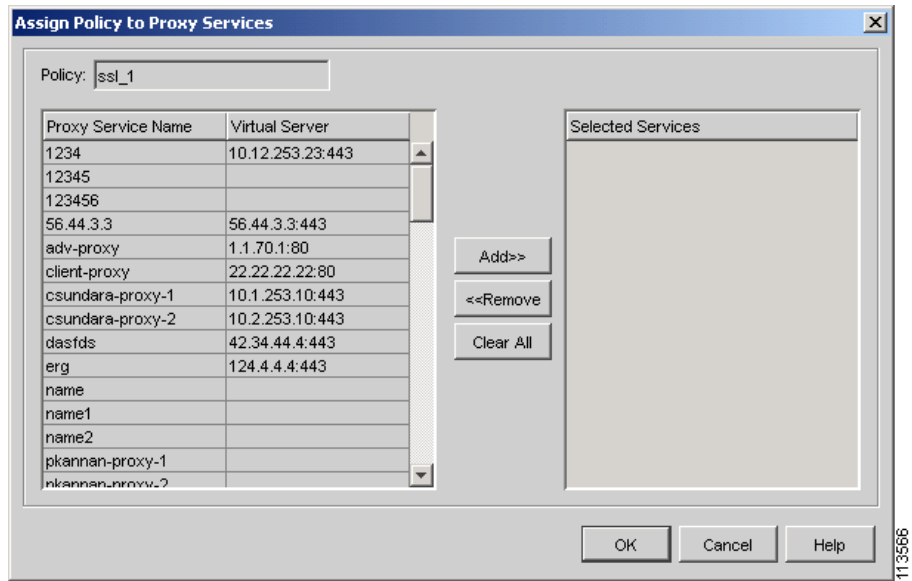
Fields	Description
Status	The status of the proxy server.
Certificate	Status of the certificate associated with the proxy service.

Assigning Policies to Proxy Services

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select a Policy from the object selector. The policy information appears on the page.
- Step 3** Select a policy from the Policies table, then click **Assign to Proxy Services**. The Assign Policy to Proxy Services dialog box appears with the following details:

Field	Description
Policy	The name of the selected policy.
Proxy Service Name	Name of the proxy service.
Client Side (Virtual)	Name of the virtual server configured for the proxy service.
Selected Services	The list of services to which the policy is associated. The list appear only after adding proxy services for the policies.

Figure 8-2 Assigning Policies to Proxy Service



Step 4 Select a Proxy Service Name, then click **Add >>** to add the policy to the selected service.

You can remove the a proxy service from the list. Select a service from the list, then click **<< Remove**.

You can clear all the services selected for assigning to a policy. Select a service from the list, then click **Clear All**.

Step 5 Click **OK** to complete the task.

Adding TCP Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **TCP Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Add**. The Add TCP Policy dialog box appears.

Field	Description
Policy	
Policy Name	Enter a name for the TCP Policy.
MSS	Enter the maximum segment size (MSS), in bytes, that the connection will identify in the SYN packet that it generates. The default is 1460 bytes. The valid range is from 256 to 2460 bytes.
Timers	
Syn Timeout	Enter the connection establishment timeout. The default is 75 seconds. The valid range is from 5 to 75 seconds.
Inactivity Timeout	Enter the amount of time, in seconds, that an established connection can be inactive. The default is 600 seconds. The valid range is 0 to 960 seconds (0 = disabled).
Reassembly Timeout	Enter the amount of time, in seconds, before the reassembly queue is cleared. If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. The default is 60 seconds. The valid range is 0 to 960 seconds (0 = disabled).

Field	Description
Fin-wait Timeout	Enter the FIN wait timeout in seconds. The default value is 600 seconds. The valid range is from 75 to 600 seconds.
Buffer Share	Enter the maximum receive buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.
Buffer Share Rx	Enter the maximum transmit buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.

Step 4 Click **OK** to add the new TCP Policy.

Editing TCP Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **TCP Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Edit**. The Add TCP Policy dialog box appears.

Field	Description
Policy	
Policy Name	Name of the TCP Policy
MSS	Modify the maximum segment size (MSS), in bytes, that the connection will identify in the SYN packet that it generates. The default is 1460 bytes. The valid range is from 256 to 2460 bytes.

Field	Description
Timers	
Syn Timeout	Modify the connection establishment timeout. The default is 75 seconds. The valid range is from 5 to 75 seconds.
Inactivity Timeout	Enter the amount of time, in seconds, that an established connection can be inactive. The default is 600 seconds. The valid range is 0 to 960 seconds (0 = disabled).
Reassembly Timeout	Enter the amount of time, in seconds, before the reassembly queue is cleared. If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. The default is 60 seconds. The valid range is 0 to 960 seconds (0 = disabled).
Fin-wait Timeout	Enter the FIN wait timeout in seconds. The default value is 600 seconds. The valid range is from 75 to 600 seconds.
Buffer Share	Enter the maximum receive buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.
Buffer Share Rx	Enter the maximum transmit buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.

Step 4 Click **OK** to save the new configuration for the TCP policy.

Deleting TCP Policy

-
- Step 1** Click **Setup** from the task bar.
 - Step 2** Click **Policies** from the left-most pane, then select **TCP Policy** from the object selector. The policy information appears on the page.
 - Step 3** Select a Policy from the list, then click Delete.
-

SSL Policy

The SSL policy option allows you to define parameters associated with the SSL stack.

If you do not associate an SSL policy with a particular proxy server, the proxy server enables all the supported cipher suites and protocol versions by default.

Viewing SSL Policy

-
- Step 1** Click **Setup** from the task bar.
 - Step 2** Click **Policies** from the left-most pane, then select **SSL Policy** from the object selector. The policy information appears on the page.

Field	Description
SSL Policies	
Policy Name	The name of the SSL policy.
Number of Proxy Services (Use Count)	Number of proxy services using the SSL Policy.

Select a policy from the SSL Policies table, then Click **Policy** Tab to view the policy details or click **Associated Proxy Services** tab to view the proxy services associated with the policies

Select a policy, then click **Assign to Proxy Services** to assign a policy to the proxy services.

Click **Add** to add a TCP policy. The Add TCP Policy dialog box appears.

Select a policy, then click **Edit** to edit a TCP policy. The Edit TCP Policy dialog box appears.

Select a policy, then click **Delete** to delete the policy.

SSL Policy Details

Field	Description
Policy	
Version	The version of the SSL to one of the following: <ul style="list-style-type: none"> • ALL—Both SSL3 and TLS 1 versions are used. • SSL3—SSL version 3 is used. • TLS1—TLS version 1 is used.
Close Protocol	Indicates whether the SSL close-protocol behavior is present.
Session Cache	Indicates whether the session caching is enabled.
Handshake Timeout (secs)	The amount of time the module keeps the connection in handshake phase.
Absolute	Indicates whether the values should be absolute values.
Session Timeout (secs)	The amount of time the module waits for the session timeout.
Cipher Suites	The list of cipher-suites acceptable to the proxy server.
Associated Proxy Services	
Name	Name of the proxy service.
Type	Type of the proxy service. For example: Server Proxy.

Field	Description
Side	The side to which the policy is applied.
Client Side (Virtual)	The IP address of the virtual server.
Server	The IP address of the server.
Oper Status	Indicates the operational status of the proxy service.
Status	Indicates the status of the proxy service.
Certificate	Status of the certificate associated with the proxy.

Adding SSL Policies

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** on the left-most pane, then select **SSL Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Add**. The Add SSL Policy dialog box appears.

Field	Description
Policy	
Policy Name	Enter a name for your new SSL Policy.
Version	Select a version for the SSL Policy. Values are: <ul style="list-style-type: none"> • ALL—Both SSL3 and TLS1 versions are used. • SSL3—SSL version 3 is used. • TLS1—TLS version 1 is used.

Field	Description
Close Protocol	Indicate whether to use an SSL close protocol. Values are: <ul style="list-style-type: none">• SSL close protocol is not followed• Follow strict SSL close protocol.
Handshake Timeout (Secs)	Enter the handshake timeout in seconds. Valid values are from 0 to 65535 seconds.
Absolute	Indicates whether the values should be absolute values.
Session Timeout (Secs)	Enter the session timeout in seconds. Valid values are from 0 to 72000 seconds.
Absolute	Select the check-box to view the absolute values.
Session Cache	Select Enabled to enable session cache. You can decide not to cache the session by selecting Disabled.

Field	Description
Session Cache Size	The size of the Session Cache. Select Absolute check-box to view the absolute value.
Cipher Suite	Select the cipher-suite from the list. The Cipher-suites that are acceptable to the proxy-server are: <ul style="list-style-type: none"> • RSA_WITH_3DES_EDE_CBC_SHA—RSA with 3des-sha. • RSA_WITH_DES_CBC_SHA—RSA with des-sha. • RSA_WITH_RC4_128_MD5—RSA with rc4-md5. • RSA_WITH_RC4_128_SHA—RSA with rc4-sha. • all—All supported ciphers.

Step 4 Click **OK** to add the new SSL Policy.

Editing SSL Policies

- Step 1** Click **Setup** from the task bar.
- Step 2** Click Policies from the left-most pane, then select **SSL Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Edit**. The Edit SSL Policy dialog box appears.

Field	Description
Policy	
Policy Name	Enter a name for your new SSL Policy.

Field	Description
Version	Select a version for the SSL Policy. Values are: <ul style="list-style-type: none">• ALL—Both SSL3 and TLS1 versions are used.• SSL3—SSL version 3 is used.• TLS1—TLS version 1 is used.
Close Protocol	Indicate whether to use an ssl close protocol. Values are: <ul style="list-style-type: none">• SSL close protocol is not followed• Follow strict SSL close protocol.
Handshake Timeout (Secs)	Enter the handshake timeout in seconds. Valid values are from 0 to 65535 seconds.
Session Timeout (Secs)	Enter the session timeout in seconds. Valid values are from 0 to 72000 seconds.
Session Cache	Select Enabled to enable session cache. You can decide not to cache the session by selecting Disabled .

Field	Description
Session Cache	Select Enabled to enable session cache. You can decide not to cache the session by selecting Disabled .
Cipher Suite	<p>Select the cipher-suite from the list.</p> <p>The Cipher-suites that are acceptable to the proxy-server are:</p> <ul style="list-style-type: none"> • RSA_WITH_3DES_EDE_CBC_SHA—RSA with 3des-sha • RSA_WITH_DES_CBC_SHA—RSA with des-sha • RSA_WITH_RC4_128_MD5—RSA with rc4-md5 • RSA_WITH_RC4_128_SHA—RSA with rc4-sha • all—All supported ciphers

Step 4 Click **OK** to apply the new values.

Deleting SSL Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **SSL Policy** from the object selector. The policy information appears on the page.
- Step 3** Select a Policy from the list, then click **Delete**.

HTTP Header Insertion Policy

HTTP header insertion is performed for the following methods: GET, HEAD, PUT, TRACE, POST, DELETE. HTTP header insertion is not performed for the CONNECT method.

**Note**

You can configure up to 100 HTTP header insertion policies, each policy consisting of up to 32 prefixes or headers. Prefix and custom headers can include up to 240 characters.

You can insert the following header types:

- **Client Certificate Headers**--Allow the backend server to see the attributes of the client certificate that the SSL module has authenticated and approved. Client certificate headers are sent only once per session. The server is expected to cache these values using the session ID, which is also inserted with the headers. In subsequent requests, the server uses the session ID to look up the cached client certificate headers on the server itself.

If the client does not send a certificate, the SSL handshake fails. There is no data phase or header insertion.

- **Client IP and Port Address Headers**

Network address translation (NAT) changes the client IP address and destination TCP port number information. When you specify Client IP Port, the SSL module inserts the client IP address and TCP destination port information in the HTTP header, allowing the server to see the client IP address and destination port number.

- **Custom Headers**

When you specify a custom string, the SSL module inserts the user-defined header verbatim in the HTTP header. You can configure up to 16 custom headers per HTTP header policy. The custom string can include up to 240 characters.

- **Prefix**

The SSL module adds the specified prefix to every inserted HTTP header. Adding a prefix enables the server to identify connections as coming from the SSL module, and not from other appliances. A prefix is not added to standard HTTP headers from the client. The *prefix_string* can be up to 240 characters.

- SSL Session Headers-- including the session ID, are used to cache client certificates based on the session ID. Session headers are also cached based on the session ID if the server wants to track connections based on a particular cipher suite. The SSL module inserts the full session headers in the HTTP request during full SSL handshake, but inserts only the session ID when the session resumes.

When you configure the SSL module as a client, the SSL module inserts the session ID of the connection between the module and the backend SSL server.

Viewing HTTP Header Insertion Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **HTTP Header Insertion Policies** from the object selector. The policy information appears on the page. The following fields appear:

Fields	Description
Policy Name	Name of the policy.
Use Count	Number of proxy services using the policy.

Select a policy from the HTTP Header Insertion Policy table, then click **Policy Tab** to view the policy details or click **Associated Proxy Services** tab to view the proxy services associated with the policies

Select a policy, then click **Assign to Proxy Services** to assign a policy to the proxy services.

Click **Add** to add a new TCP policy. The Add TCP Policy dialog box appears.

Select a policy, then click **Edit** to edit a TCP policy. The Edit TCP Policy dialog box appears.

Select a policy, then click **Delete** to delete the policy.

Fields	Description
Policy	
Policy Name	The name of the policy.
General	
Prefix	The prefix or the type of header.
Client Certificate Insertion	Indicates whether the client certificate insertion is enabled.
Client Ip Port Insertion	Indicates whether the client IP Port insertion is enabled.
Session Header Insertion	Indicates whether the Session Header insertion is enabled.
Custom Headers	
Header Name	The user-defined header verbatim in the HTTP header.
Value	Value of the header.
Associated Proxy Services	
Name	The name of the proxy service associated with the policy.
Type	The type of the proxy service. Example: Server Proxy.
Virtual Server	The IP address of the virtual server.
Server	The IP address of the server.
Oper Status	The operational status of the service.
Status	The status of the proxy service.
Certificate	The status of the certificate associated with the proxy service.

Adding HTTP Header Insertion Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **HTTP Header Insertion Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Add**. The Add HTTP Header Insertion Policy dialog box appears:

Field	Description
Policy	
Policy Name	Enter a name for your new policy.
Prefix	Enter a prefix to be used with the policy. For example: cisco.com
Client Certificate Insertion	Select Enabled to enable the client certificate insertion.
Client IP Port Insertion	Select Enabled to enable the client IP port insertion.
Session Header Insertion	Select Enabled to enable Session Header Insertion.
Custom Headers	
Header	The user-defined header verbatim in the HTTP header. You can include up to 16 custom headers per HTTP header policy. Click Add to add the header name.
Value	Enter a header name, then enter the value. Click Add to add a value to the header.

- Step 4** Click **OK** to add the new policy.

Editing HTTP Header Insertion Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **HTTP Header Insertion Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Edit**. The Edit HTTP Header Insertion Policy dialog box appears:

Field	Description
Policy	
Policy Name	Name of the policy.
Prefix	Modify the existing prefix or you can enter a new prefix.
Client Certificate Insertion	Select Enabled to enable the client certificate insertion.
Client IP port Insertion	Select Enabled to enable the client IP Port insertion.
Session Header Insertion	Select Enabled to enable the Session Header insertion.
Custom Headers	
Header	The user-defined header verbatim in the HTTP header. You can configure up to 16 custom headers per HTTP header policy.
Value	Enter the value.

- Step 4** Click **OK** to apply the modifications.

Deleting HTTP Header Insertion Policy

-
- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **HTTP Header Insertion Policy** from the object selector. The policy information appears on the page.
- Step 3** Select a Policy from the list, then click Delete.
-

URL Rewrite Policy

The URL rewrite feature supports the rewriting of redirection links. The system scans only the Location: HTTP header field in the response from the server and rewrites the rules accordingly. The URL rewrite feature does not support embedded links.

The URL rewrite feature rewrites the protocol and the non-default port (default ports are port 80 for cleartext and port 443 for SSL).

**Note**

You can configure up to 100 URL rewrite policies, each policy consisting of up to 32 rewrite rules per SSL proxy service, up to 200 characters per rule.

Follow these guidelines for URL rewrite:

- An exact URL match takes precedence over a wildcard rule. A suffix wildcard rule takes precedence over a prefix wildcard rule.

For example, **www.cisco.com** takes precedence, then **www.cisco.***, then ***.cisco.com**.
- Enter only one suffix or prefix wildcard rule at one time. For example, do not enter **www.cisco.*** and **www.cisco.c*** in the same policy. Similarly, do not enter ***w.cisco.com** and ***.cisco.com** in the same policy.
- Do not enter two exact URL match rules in the same policy. For example, do not enter **www.cisco.com clearport 80 sslport 443** and **www.cisco.com clearport 81 sslport 444** in the same policy. In this case, the second rule entered overwrites the first rule.

- URL rewrite is performed for both offload and backend (HTTP-to-HTTPS, and HTTPS-to-HTTP). This includes port rewrites.

Viewing URL Rewrite Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **URL Rewrite Policy** from the object selector. The policy information appears on the page.

The following fields appear:

Fields	Description
Policy Name	The name of the URL-Rewrite policy.
Number of Proxy Services (Use Count)	Number of proxy services using the SSL Policy.

Select a policy from the URL Rewrite Policy table, then Click **Policy** Tab to view the policy details or click **Associated Proxy Services** tab to view the proxy services associated with the policies

Select a policy, then click **Assign to Proxy Services** to assign a policy to the proxy services.

Click **Add** to add a URL Rewrite Policy. The Add URL Rewrite Policy dialog box appears.

Select a policy, then click **Edit** to edit a URL Rewrite Policy. The Edit URL Rewrite Policy dialog box appears.

Select a policy, then click **Delete** to delete the policy.

Following are the URL Rewrite Policy details:

Fields	Description
Policy	
Policy Name	Name of the selected policy.
URL Host String	The host string of the URL.
HTTP Port	The HTTP port to be used for the traffic.
HTTPS Port	The HTTPS port to be used for the traffic.
Associated Proxy Services	
Name	The name of the associated proxy service.
Type	The type of the proxy service. For example: Server Proxy.
Client Side	The IP address of the virtual server.
Server	The IP address of the server.
Oper Status	The operational status of the server.
Certificate	Status of the certificate associated with the proxy service.

Adding URL Rewrite Policy

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Policies** from the left-most pane, then select **URL Rewrite Policy** from the object selector. The policy information appears on the page.
- Step 3** Click **Add**. The Add URL Rewrite Policy dialog box appears.

Field	Action/Description
Policy Name	Enter a name for the policy.
URL Host String	The host string of the url.
HTTP Port	The HTTP Port to be used for the traffic.
HTTPS Port	The HTTPS port to be used for the traffic.
URL Host String	Enter the URL host string for rewriting, then click Add to create the new URL Rewrite Rule.
HTTP Port	(Optional) Enter the clear port value. The HTTP port specifies the port portion of the URL to be rewritten. If you do not enter a value, the default value is used.
HTTPS Port	(Optional) Enter the HTTPS port value. The HTTPS port specifies the port portion of the URL that should be rewritten.If you do not enter a value, the default value is used.

You can specify URL alone. But you cannot add clear port and SSL port without entering a URL value.



Note You can configure up to 32 rewrite rules per SSL proxy service, up to 240 characters per rule. You should enter only one suffix or prefix wildcard character (*) only once per rewrite rule.

To remove a URL Rewrite Rule, select the rule from the table, then click **Remove**.

Step 4 Click **OK** to add the new policy.

Editing URL Rewrite Policy

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies** from the left-most pane, then select **URL Rewrite Policy** from the object selector. The policy information appears on the page.

Step 3 Select a policy, then click **Edit**. The Edit URL Rewrite Policy dialog box appears.

The following fields appear:

Field	Action/Description
Policy Name	Enter a name for the policy.
URL Host String	The host string of the url.
HTTP Port	The HTTP Port used for the traffic.
HTTPS Port	The HTTPS port used for the traffic.
URL Host String	Enter the URL for rewriting, then click Add to create the new URL Rewrite Rule.

Field	Action/Description
HTTP Port	(Optional) Enter the clear port value. The HTTP port specifies the port portion of the URL to be rewritten. If you do not enter a value, the default value is used.
HTTPS Port	(Optional) Enter the HTTPS port value. The HTTPS port specifies the port portion of the URL that should be rewritten. If you do not enter a value, the default value is used

You can specify URL alone. But you cannot add Clear Port and SSL Port without entering a URL value.



Note You can configure up to 32 rewrite rules per SSL proxy service, up to 240 characters per rule. You should enter only one suffix or prefix wildcard character (*) only once per rewrite rule.

To remove a URL Rewrite Rule, select the rule from the table, then click **Remove**.

Step 4 Click **OK** to modify values.

Viewing URL Rules and Outcome

The URL Rules and Outcome dialog box helps you view the URL rules you have set and the outcome of the rules.

To view URL Rules and Outcome:

-
- Step 1** Click **Setup** from the task bar.
 - Step 2** Click **Policies** from the left-most pane, then select **URL Rewrite Policy** from the object All Router View. The policy information appears on the page.
 - Step 3** Select a policy from the table. The details appear on the URL Rewrite Policy Details pane. If you have set a URL rewrite for the policy, The View Rules and Outcome button will be active.
 - Step 4** Click **View Rules and Outcome**. The Rules and Outcome dialog box appears.
To view rules and outcome for server proxy, Click **Rules and Outcome for Client Proxy** tab. The following fields appear:

Field	Action/Description
URLs that Match	URL match criterion.
URL Rewrite	The new URL.

To view rules and outcome for server proxy, Click **Rules and Outcome for Server Proxy** tab. The following fields appear:

Field	Action/Description
URLs that Match	URL match criterion.
URL Rewrite	The new URL.

Deleting URL Rewrite Policy

To delete a policy:

-
- Step 1** Click **Setup** from the task bar.
 - Step 2** Click **Policies** from the left-most pane, then select **URL Rewrite Policy** from the object selector. The policy information appears on the page.
 - Step 3** Select a Policy from the list, then click **Delete**.
-



Managing VLANs

The SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.

VLAN IDs must be the same for the switch and the module.



Note

When you create VLANs using CVDM-SSLM, you must ensure that the corresponding VLANs exist on the switch and configured to permit the SSL VLANs.

The following topics are described in this section:

- [Viewing VLANs, page 9-2](#)
- [Adding VLANs, page 9-3](#)
- [Editing VLANs, page 9-4](#)
- [Deleting VLANs, page 9-4](#)

Viewing VLANs

To view VLANs configured on the module:

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **VLANs** in the left-most pane. The VLAN page appears.
 - Step 3** Click VLANs group folder in the object selector.

The following fields appear:

Field	Description
VLAN ID	Identification number for the VLAN.
IP Address / Subnet Mask	IP address or subnet mask of the VLAN.
Subnet	Subnet of the VLAN
Gateway	The gateway IP address of the VLAN
Route	
Destination	Destination IP address.
Next Hop	Next Hop IP address.

Click **Add...** to add a new VLAN.

To edit the VLAN settings, select a VLAN from the table, then click **Edit...**

To delete a VLAN, select a VLAN from the table, then click **Delete**.

Adding VLANs

- Step 1** Click **Setup** in the task bar.
- Step 2** Click **VLANs** in the left-most pane. The VLAN page appears.
- Step 3** Click VLANs group folder in the object **Selector**.
- Step 4** Click **Add...**

The following fields appear:

Field	Description
VLAN ID (2 - 1005)	Enter the VLAN ID. The value should be between 2 and 1005.
IP Address	Enter the VLAN IP address.
Net Mask	Select the mask for the IP address. Values are: <ul style="list-style-type: none"> • 255.0.0.0 • 255.255.0.0 • 255.255.255.0
Gateway	Enter the IP address of the gateway.
Route	
Destination IP Address	Enter the IP address of the destination.
Destination Netmask	Enter the mask for the destination.

- Step 5** Click **OK** to add the new VLAN.

Editing VLANs

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **VLANs** in the left-most pane. The VLAN page appears.
 - Step 3** Click **VLANs** group folder in the object selector.
 - Step 4** Click **Edit...**

The following fields appear:

Field	Description
VLAN ID	The ID of the VLAN you have selected.
IP Address	Modify the IP address of the VLAN.
Mask	Modify the mask to be used for the VLAN.
Gateway	Modify the IP address of the gateway.
Route	
Destination IP Address	Enter the destination IP address.
Destination Netmask	Enter the destination netmask.

- Step 5** Click **OK** to apply the changes.
-

Deleting VLANs

-
- Step 1** Click **Setup** in the task bar.
 - Step 2** Click **VLANs** in the left-most pane. The VLAN page appears.
 - Step 3** Click **VLANs** group folder in the object selector.
 - Step 4** Click **Delete**.
-



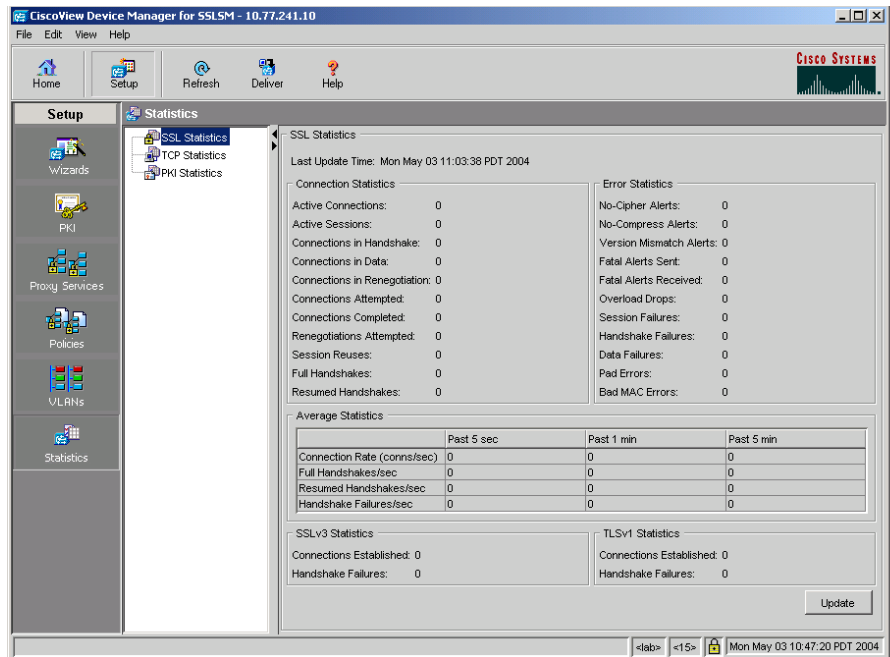
Viewing Statistics

CVDM-SSLSM allows you to view the statistics of the traffic through the SSL Module. The values are not auto-refreshed. You can manually refresh the values.

CVDM-SSLSM provides statistical information on the following:

- [TCP Statistics, page 10-2](#)
- [SSL Statistics, page 10-4](#)
- [PKI Statistics, page 10-13](#)

Figure 10-1 Statistics Page



113575

TCP Statistics

To view TCP Statistics:

- Step 1** Click **Setup** in the task bar, then select **Statistics** from the left-most pane.
- Step 2** Select **TCP Statistics** from the Object Selector.

The following fields appear:

Field	Description
Last Update Time	The time at which the statistics information was last updated.
Show Counter Value Change (Delta)	<p>Values are:</p> <p>Delta—Select this option to view the counter value change (delta) between subsequent updates. When this option is selected, the measurement period between subsequent updates will be displayed.</p> <p>Absolute—Displays the cumulative value.</p>
Connection Statistics	
Connections in Established State	Number of connections in ESTABLISHED state.
Current in TIME-WAIT State	Number of connections in TIME-WAIT state.
Connections Initiated	Number of TCP connections initiated by the SSLSM.
Connections Dropped	Number of connections that were dropped.
Connections Closed	Number of connections that were closed.
Connections Accepted	Number of TCP connections accepted by the SSLSM.

Click **Update** to refresh the values.

SSL Statistics

To view SSL Statistics:

-
- Step 1** Click **Setup** in the task bar, then select Statistics from the left-most pane.
 - Step 2** Select **SSL Statistics** from the Object [Selector](#).

The following fields are displayed:

Field	Description
Last Update Time	The time at which the statistics information was last updated.
Show Counter Value Change (Delta)	<p>Values are:</p> <p>Delta—Select this option to view the counter value change (delta) between subsequent updates. When this option is selected, the measurement period between subsequent updates will be displayed.</p> <p>Absolute—Displays the cumulative value.</p>
Connection Statistics	
Active Connections	Number of Active SSL connections
Active Sessions	Number of Session IDs in use.
Connections in Handshake	Number of connections in the Handshake phase.
Connections in Data	Number of connections in data phase.
Connections in Renegotiation	Number of connections in re-negotiation phase.
Connections Attempted	Number of connections attempted.
Connections Completed	Number of connections that were completed.
Renegotiations Attempted	Number of re-negotiations attempted.
Session Reuses	Number of times when the session got reused.
Full Handshakes	Number of Full Handshakes performed.
Resumed Handshakes	Number of resumed handshakes performed.
Error Statistics	

Field	Description
No-Cipher Alerts	Number of Handshake Failure alerts sent due to unsupported Cipher suites
No-Compress Alerts	Number of Handshake Failure alerts sent due to unsupported compression scheme.
Version Mismatch Alerts	Number of Handshake Failure alerts sent due to unsupported SSL version.
Fatal Alerts Sent	Number of fatal alerts sent.
Fatal Alerts Received	Number of fatal alerts received.
Overload Drops	Number of connections that were declined due to overload.
Session Failures	Number of instances when the allocation failed.
Handshake Failures	Number of connections that failed in the Handshake phase.
Data Failures	Number of connections that failed due to data errors (Pad Error/Bad MAC Error)
Pad Errors	Number of SSL records received with error in padding.
Bad MAC Errors	Number of SSL records received with Bad MAC.
Average Statistics	
Connection Rate (conns/sec)	Number of connections in a second.
Full Handshakes/sec	Number of handshakes in a second.
Resumed Handshakes/sec	Number of handshakes resumed in a second.
Handshake Failures/sec	Number of handshake failures in a second.
SSLv3 Statistics	
Connections Established	Number of SSLv3 connections established.

Field	Description
Handshake Failures	Number of SSLv3 handshakes failed.
TSLv1 Statistics	Number of TSLv1 connections.
Connections Established	Number of connections established.
Handshake Failures	Number of handshakes failed.
Timeout Statistics	
SYN Timeouts	Number of SYN Timeouts.
Idle Timeouts	Number of Idle Timeouts.
Reassembly Timeouts	Number of Reassembly Timeouts.
FIN-WAIT2 Timeouts	Number of FIN-WAIT2 Timeouts.
Drop Statistics	
Invalid MSS Drops	Connections dropped due to unsupported MSS size.
Connection Buffer Pool Drops	Number of connection buffer pool drops.
Packet Statistics (Transmit)	
Total Packets	Number of packets transmitted
Data Packets	Number of data packets transmitted.
Retransmitted Packets	Number of packets retransmitted.
Packet Statistics (Receive)	
Total Packets	Number of packets received
Packets in Sequence	Number of packets received in sequence.
Packets out of sequence	Number of packets received out of sequence.

Click **Clear** to clear the counter values on the SSLSM.

Click **Update** to refresh the values from the SSLSM.

Proxy SSL Statistics Summary

You can view a summary of the statistics for the client and server proxy.

To view Proxy Service Statistics Summary:

-
- Step 1** Click **Setup** in the task bar, then select Statistics from the left-most pane.
 - Step 2** Select **SSL Statistics > Client Proxy** or **Server Proxy** from the Object [Selector](#).
 - Step 3** Click the **Summary** tab.

The following fields are displayed:

Field	Description
Last Update Time	The time at which the statistics information was last updated.
Show Counter Values Change (Delta)	Values are: Delta—Select this option to view the counter value change (delta) between subsequent updates. When this option is selected, the measurement period between subsequent updates will be displayed. Absolute—Displays the cumulative value.

The table displays the following details:

Field	Description
Proxy Service	The name of the proxy service.
Connections	
Attempted	Number of connected attempted.
Completed	Number of completed connections.
Active	Number of active connections.
Errors	
Fatal Alarms	Number of Fatal Alarms.
Handshake Failures	Number of handshake failures.
Throughput (bytes)	
Encrypted	Number of encrypted bytes.
Decrypted	Number of decrypted bytes.

Click **Clear** to clear the counter values on the SSLSM.

Click **Update** to refresh the values from the SSLSM.

Proxy SSL Statistics - Proxy Services

You can view the statistics for the proxy service (client proxy and service proxy).

To view Proxy Service Statistics:

-
- Step 1** Click **Setup** in the task bar, then select Statistics from the left-most pane.
 - Step 2** Select **SSL Statistics > Client Proxy or Server Proxy** from the Object **Selector**.
 - Step 3** Select any of the proxy service from the list of configured proxy services.
The following fields are displayed:

Field	Description
Last Update Time	The time at which the statistics information was last updated.
Show Counter Value Change	Values are: Delta—Select this option to view the counter value change (delta) between subsequent updates. When this option is selected, the measurement period between subsequent updates will be displayed. Absolute—Displays the cumulative value.

The table displays the following details:

Field	Description
Proxy Service	The name of the proxy service. Click the proxy service name to view the details of the selected proxy service
Connections	
Attempted	Number of connected attempted.
Completed	Number of completed connections.
Active	Number of active connections.
Errors	
Fatal Alarms	Number of Fatal Alarms.
Handshake Failures	Number of handshake failures.
Throughput (bytes)	
Encrypted	Number of encrypted bytes.
Decrypted	Number of decrypted bytes.

Click **Clear** to clear the counter values on the SSLSM.

Click **Update** to refresh the values from the SSLSM.

Proxy Service SSL Statistics

You can view the statistics for a single proxy service (client proxy and service proxy).

To view Proxy Service Statistics:

- Step 1** Click **Setup** in the task bar, then select Statistics from the left-most pane.
- Step 2** Select **SSL Statistics > Client Proxy or Server Proxy** from the Object [Selector](#).
- Step 3** Select any of the proxy service from the list of configured proxy services.

The following fields are displayed:

Field	Description
Connection Counters	
Connections Attempted	Number of connections attempted.
Connections Completed	Number of connections that were completed.
Full Handshakes	Number of Full Handshakes performed.
Resumed Handshakes	Number of resumed handshakes performed.
Active Connections	
Connections in Handshake	Number of connections in the Handshake phase.
Connections in Data	Number of connections in data phase.
Connections in Renegotiation	Number of connections in re-negotiation phase.
Valid Sessions	Number of valid sessions.
Errors	
Handshake Failures	Number of handshake failures.
Data Failures	Number of data failures.
Fatal Alerts Sent	Number of fatal alerts sent.
Fatal Alerts Received	Number of fatal alerts received.

Field	Description
No-cipher Alerts	Number of no cipher alerts.
No-compress Alerts	Number of no compress alerts.
Version Mismatch Alerts	Number of version mismatch alerts.
Bad MAC Received	Number of SSL records received with Bad MAC.
Pad Errors	Number of SSL records received with error in padding.
Session Limit Exceeds	
Throughput	
Bytes Encrypted	Number of bytes encrypted.
Bytes Decrypted	Number of bytes decrypted.

Click **Clear** to clear the counter values on the SSLSM.

Click **Update** to refresh the values from the SSLSM.

PKI Statistics

To view PKI Statistics:

Step 1 Click **Setup** in the task bar, then select **Statistics** from the left-most pane.

Step 2 Select **PKI Statistics** from the Object [Selector](#).

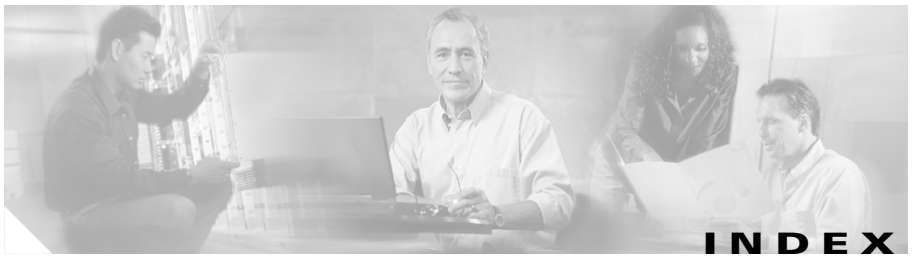
The following fields are displayed:

Field	Description
Last Update Time	The time at which the statistics information was last updated.
Valid Signatures	Number of valid signatures.
Invalid Signatures	Number of invalid signatures.

Field	Description
Invalid Certificates	Number of invalid certificates.
Authentications with Warning (No CRL Check)	Number of authentications with warning.
Number of CRL Polling	Number of CRL polling.
Requests with no Peer Certificate	Number of requests received with no peer certificate.
CRL Query Failures	Number of CRL queries failed.
Unauthorized Requests	Number of unauthorized requests.
No Certificate Chain	Number of requests without certificate chains.
Root Certificate not Self-signed	Number of root certificates without self-signature.
No DER Encoded Certificate	Number of Certificates without DER encoding.
<hr/>	
No Memory	Number of certificates failures due to lack of memory.
Bad DER Certificate Length	Number of certificates with bad DER certificate length.
Failed to get Key from Certificate	Number of requests that failed to get a key from the certificate.

Click **Clear** to clear the counter values on the SSLSM.

Click **Update** to refresh the values from the SSLSM.



A

- action buttons, understanding [1-20](#)
- audience for this document [xiii](#)

C

- CA pools (see client certificate authentication, managing) [5-1](#)
- certificate ACLs, managing [6-1](#)
 - adding [6-5](#)
 - assigning to trustpoints [6-4](#)
 - deleting [6-9](#)
 - editing [6-7](#)
 - viewing associated trustpoints [6-5](#)
- certificates, managing [3-1](#)
 - Certificate wizard [3-10](#)
 - CA certificate [3-19](#)
 - certificate requests [3-25](#)
 - certificate trustpoint, configuring using [3-12](#)
 - configure enrollment parameters [3-17](#)
 - launching [3-11](#)
 - proxy certificate attributes [3-16](#)
 - SSL module, delivering configuration to [3-25](#)
 - summary, displaying [3-24](#)
 - trustpoint configuration status, viewing [3-25](#)
 - trustpoints and RSA key pairs, configuring using [3-15](#)
 - trustpoint setup tasks [3-24](#)
 - challenge password [3-75](#)
 - deleting [3-74](#)
 - editing [3-68](#)
 - importing and exporting [3-26](#)
 - exporting using the wizard [3-38](#)
 - importing from external PKI system [3-26](#)
 - scenarios [3-75](#)
 - trustpoint details [3-58](#)
 - authentication [3-65](#)
 - authentication and enrollment [3-66](#)
 - enrollment [3-65](#)
 - export [3-68](#)
 - import of a proxy [3-66](#)
 - renewal [3-67](#)
 - viewing certificates [3-54](#)
- CLI commands, delivering to the device [1-22](#)
- client certificate authentication, managing [5-1](#)
 - adding CA pools [5-5](#)
 - assigning CA pools to proxy services [5-4](#)
 - deleting CA pools [5-7](#)

editing CA pools [5-6](#)
 scenarios [5-7](#)
 viewing CA pools [5-2](#)

configuring

keys and certificates for PKI [2-2](#)
 PKI [2-1](#)

D

desktop, understanding [1-7](#)
 documentation [xiv](#)
 audience for this [xiii](#)
 related to this product [xv](#)
 typographical conventions in [xiii](#)

G

getting started [1-1](#)
 action buttons, understanding [1-20](#)
 CLI commands, delivering to the device [1-22](#)
 desktop, understanding [1-7](#)
 key features [1-4](#)
 policies [1-4](#)
 proxy service [1-4](#)
 public key infrastructure [1-4](#)
 statistics [1-3, 1-4](#)
 navigation [1-6](#)
 preferences, modifying [1-21](#)
 setup [1-17](#)

starting CVDM [1-5](#)
 what's next [1-24](#)

K

key features of the product [1-4](#)
 policies [1-4](#)
 proxy service [1-4](#)
 public key infrastructure [1-4](#)
 statistics [1-3, 1-4](#)
 key pairs, managing [4-1](#)
 adding key pairs [4-4](#)
 deleting key pairs [4-6](#)
 Key Pair wizards [4-6](#)
 Key Pair Export wizard [4-10](#)
 Key Pair Import wizard [4-7](#)
 scenarios [4-16](#)
 understanding key pairs [4-1](#)
 viewing key pairs [4-2](#)

P

PKI (Public Key Infrastructure)
 about [1-4](#)
 configuring keys and certificates [2-2](#)
 configuring PKI [2-1](#)
 overview [2-1](#)
 policies, managing [8-1](#)
 HTTP Header Insertion policies [8-17](#)

- adding [8-21](#)
 - deleting [8-23](#)
 - editing [8-22](#)
 - viewing [8-19](#)
 - SSL policies [8-10](#)
 - adding [8-12](#)
 - deleting [8-16](#)
 - editing [8-14](#)
 - viewing [8-10](#)
 - TCP policies [8-3](#)
 - adding [8-7](#)
 - assigning to proxy services [8-5](#)
 - deleting [8-10](#)
 - editing [8-8](#)
 - viewing [8-3](#)
 - URL Rewrite policies [8-23](#)
 - adding [8-26](#)
 - deleting [8-30](#)
 - editing [8-27](#)
 - preferences, modifying [1-21](#)
 - proxy services, managing [7-1](#)
 - about [1-4](#)
 - NAT Pools [7-26](#)
 - adding [7-29](#)
 - assigning to proxy services [7-30](#)
 - deleting [7-30](#)
 - understanding [7-27](#)
 - viewing [7-28](#)
 - Proxy Service wizards [7-2](#)
 - Advanced [7-8](#)
 - available CA pools [7-14](#)
 - available NAT pools [7-13](#)
 - Basic [7-3](#)
 - scenarios [7-32](#)
 - viewing [7-15](#)
 - viewing proxy services details [7-18](#)
 - Proxy Service Wizards [7-2](#)
-
- S**
- setup [1-17](#)
 - starting CVDM [1-5](#)
 - statistics, viewing [10-1](#)
 - PKI statistics [10-13](#)
 - SSL statistics [10-4](#)
 - TCP statistics [10-2](#)
-
- T**
- typographical conventions in this document [xiii](#)
-
- V**
- viewing, certificate ACL [6-2](#)
 - VLANs, managing [9-1](#)
 - adding [9-3](#)
 - deleting [9-4](#)

editing [9-4](#)

viewing [9-2](#)