



# Cisco 11000 Series Secure Content Accelerator Configuration Guide

August, 2002

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: 78-13124-04

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.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0201R)

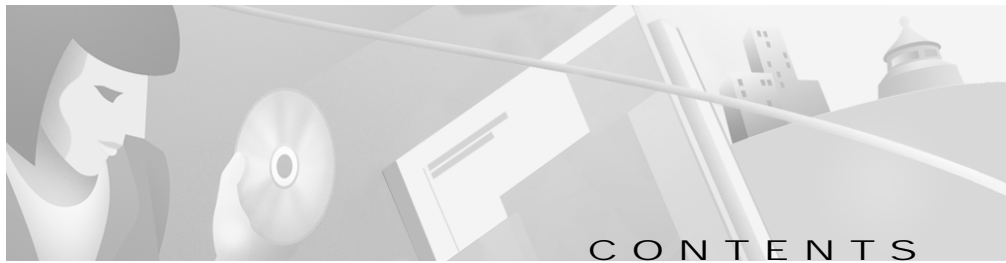
This product includes cryptographic software written by Eric A. Young. This product includes software written by Tim J. Hudson.

*Cisco 11000 Series Secure Content Accelerator Configuration Guide*

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.





# CONTENTS

## **About This Guide xxxi**

How to Use This Guide xxxi

Symbols and Conventions xxxiii

Obtaining Documentation xxxiv

World Wide Web xxxiv

Documentation CD-ROM xxxiv

Ordering Documentation xxxv

Documentation Feedback xxxv

Obtaining Technical Assistance xxxvi

Cisco.com xxxvi

Technical Assistance Center xxxvi

Cisco TAC Web Site xxxvii

Cisco TAC Escalation Center xxxviii

---

## CHAPTER 1

### **Overview 1-1**

Product Overview 1-2

Secure Content Accelerator Versions 1-3

Released Platforms 1-4

---

## CHAPTER 2

### **Installing the Hardware and Software 2-1**

Site Requirements 2-2

Required Tools and Equipment 2-2

Shipment Contents 2-2

- Unpacking the Secure Content Accelerator 2-3
- Installing the Hardware 2-3
  - Installing as a Free-Standing Unit 2-4
  - Installing as a Rack-Mounted Unit 2-5
- Panel Descriptions 2-5
  - Identifying SCA Models 2-7
- Connecting to Power 2-7
- Connecting to Ethernet 2-9
- Installing the Software 2-9
  - Linux Software 2-10
  - Solaris Software 2-10
  - Windows NT and Windows 2000 Software 2-11

CHAPTER 3

**Using the QuickStart Wizard 3-1**

- Before You Begin 3-2
- Initiating a Management Session 3-2
  - Serial Management and IP Address Assignment 3-2
  - Telnet 3-3
  - Remote Configuration Manager Application 3-4
    - Linux 3-4
    - Solaris 3-4
    - Windows NT and Windows 2000 Software 3-4
- Starting the QuickStart Wizard 3-5
  - Using a Serial or Telnet Connection 3-5
  - Using the Remote Configuration Manager 3-6
- Using the QuickStart Wizard 3-7
  - Using the QuickStart Wizard with a Configured Appliance 3-16

**Using the Configuration Manager 4-1**

Overview 4-2

Configuration Security 4-3

Passwords 4-3

Access Lists 4-4

Encrypted Management Sessions 4-4

Factory Default Reset Password 4-4

Before You Begin 4-5

Initiating a Management Session 4-5

Serial Management and IP Address Assignment 4-5

Telnet 4-7

Running the Remote Configuration Manager 4-7

Linux 4-7

Solaris 4-7

Windows NT and Windows 2000 Software 4-7

Using the Remote Configuration Manager 4-8

Specifying Devices 4-8

Working with Device Groups 4-9

Remote Configuration Caching 4-10

Configuring the Device 4-10

Example: Setting up Basic Device Parameters 4-11

Example: Setting up a Secure Server 4-12

Example: Setting up a Backend Server 4-15

Example: Setting up a Reverse-Proxy Server 4-16

Example: Configuring Secure URL Rewrite 4-17

Example: Configuring SNTP Servers 4-19

Example: Configuring Encrypted Management Sessions 4-20

- Example: Restricting Access using an Access List 4-22
- Configuring an Ethernet Interface 4-23
- Step-Up Certificates and Server-Gated Cryptography 4-23
- Configuring Certificate Groups 4-24
  - Example: Configuring a Certificate Group 4-24
  - Example: Importing Certificate Groups 4-26
- Using Client and Server Certificate Authentication 4-27
  - Example: Configuring Server Certificate Authentication 4-27
  - Example: Configuring Client Certificate Authentication 4-29
- Generating Keys and Certificates 4-30
  - Example: Generating an RSA Key 4-30
  - Example: Generating a Certificate 4-30
- Supporting SNMP 4-31
  - Example: Configuring SNMP 4-31
- Supporting RIP 4-32
  - Example: Configuring RIP 4-32
- Supporting Other Secure Protocols 4-32
  - Example: Configuring a Secure Mail Server 4-33
- Supporting FIPS 4-33

CHAPTER 5

**Graphical User Interface Reference 5-1**

- Overview 5-2
- Browser and System Support 5-2
- Enabling Web Management 5-2
- Restricting Access to Web Management 5-3
- Starting the GUI 5-3
  - Configuring for Client-Side Access 5-4



Web Management User Interface	5-5
General Configuration Examples	5-6
Example: Setting the Device Name (Hostname)	5-6
Example: Resetting the IP Address	5-7
Example: Configuring an Ethernet Interface	5-8
Example: Enabling RIP	5-9
Example: Adding a Route to the Routing Table	5-10
Example: Working with Syslogs	5-12
Example: Restricting Access using an Access List	5-13
Example: Reloading (Rebooting) the Appliance	5-16
Example: Setting an Enable Password	5-17
Example: Configuring SNMP	5-18
SSL Configuration Examples	5-21
Example: Setting up a Secure Server	5-21
Example: Creating and Using Certificate Groups	5-32
Example: Supporting Other Secure Protocols	5-35
Example: Generating an RSA Private Key	5-36
Example: Generating a Self-Signed Certificate	5-40
Example: Importing a PKCS#7 Certificate Group	5-44
Example: Importing a PKCS#12 Certificate Group	5-45
Running the Secure Server Wizard	5-46

**FIPS Operation 6-1**

FIPS Capabilities	6-2
Using FIPS Mode	6-3
Creating a Server in FIPS Mode	6-5

- Command Changes 6-7
  - Unavailable Commands 6-7
  - Differing Command Behaviors 6-7
- Returning to Normal Operation 6-9
- More Information 6-10

---

APPENDIX A

**Specifications A-1**

- Electrical Specifications A-2
- Environmental Specifications A-2
- Physical Specifications A-3

---

APPENDIX B

**Deployment Examples B-1**

- Single Device B-2
- Load Balancing B-2
- Use with the CSS B-3
  - In-Line B-4
  - Transparent Sandwich B-8
  - One-Armed Non-Transparent Proxy B-16
  - One-Armed Transparent Proxy B-22
- Connecting the Device to a Terminal Server B-30
- Web Site Changes B-31

---

APPENDIX C

**Command Summary C-1**

- Input Data Format Specification C-2
- Text Conventions C-2
- Editing and Completion Features C-3
- Command Hierarchy C-5

Configuration Security	<b>C-6</b>
Passwords	<b>C-6</b>
Access Lists	<b>C-7</b>
Encrypted Management Sessions	<b>C-7</b>
Factory Default Reset Password	<b>C-7</b>
Methods to Manage the Device	<b>C-8</b>
Initiating a Management Session	<b>C-10</b>
Serial Management and IP Address Assignment	<b>C-10</b>
Telnet	<b>C-11</b>
Running the Remote Configuration Manager	<b>C-11</b>
Linux	<b>C-11</b>
Solaris	<b>C-11</b>
Windows NT and Windows 2000 Software	<b>C-12</b>
Using the Remote Configuration Manager	<b>C-12</b>
Specifying Devices	<b>C-12</b>
Working with Device Groups	<b>C-13</b>
Remote Configuration Caching	<b>C-14</b>
Top Level Command Set	<b>C-15</b>
Non-Privileged Command Set	<b>C-15</b>
Privileged Command Set	<b>C-63</b>
Group Configuration Command Set	<b>C-85</b>
Configuration Command Set	<b>C-87</b>
Interface Configuration Command Set	<b>C-118</b>
SSL Configuration Command Set	<b>C-120</b>
Backend Server Configuration Command Set	<b>C-130</b>
Certificate Configuration Command Set	<b>C-141</b>
Certificate Group Configuration Command Set	<b>C-145</b>

- Key Configuration Command Set **C-148**
- Reverse-Proxy Server Configuration Command Set **C-153**
- Security Policy Configuration Command Set **C-161**
- Server Configuration Command Set **C-167**

---

APPENDIX D

**Troubleshooting D-1**

- Troubleshooting the Hardware **D-2**

---

APPENDIX E

**SSL Introduction E-1**

- Introduction to SSL **E-2**
- Port Blocking Mechanism **E-2**
- Before You Begin **E-4**
- Using Existing Keys and Certificates **E-4**
  - Apache mod\_SSL **E-5**
  - ApacheSSL **E-5**
  - Stronghold **E-5**
  - IIS 4 on Windows NT **E-5**
  - IIS 5 on Windows 2000 **E-6**
- Configuration Security **E-7**
  - Passwords **E-7**
  - Access Lists **E-8**
  - Encrypted Management Sessions **E-8**
  - Factory Default Reset Password **E-8**
- Cisco SSL Configuration Components **E-9**
  - Real Server IP Addresses **E-9**
  - Keys **E-9**

Certificates **E-9**

Step-Up Certificates and Server-Gated Cryptography **E-10**

Chained Certificates **E-10**

Security Policies **E-10**

Cisco Secure Content Accelerator Management **E-12**

---

APPENDIX F

**Regulatory Information 15**

Regulatory Standards Compliance **16**

Canadian Radio Frequency Emissions Statement **16**

FCC Class A **17**

CISPR 22 (EN 55022) Class A **18**

VCCI **18**

---

GLOSSARY

---

INDEX





## FIGURES

<i>Figure 2-1</i>	Secure Content Accelerator Front Panel	<b>2-6</b>
<i>Figure 2-2</i>	Secure Content Accelerator Rear Panel	<b>2-6</b>
<i>Figure 4-1</i>	Configuration Manager Hierarchy	<b>4-2</b>
<i>Figure 5-1</i>	Password Request Dialog Box	<b>5-4</b>
<i>Figure 5-2</i>	Basic User Interface Example	<b>5-5</b>
<i>Figure 5-3</i>	Changing Hostname Configuration Example	<b>5-7</b>
<i>Figure 5-4</i>	Resetting IP Information Configuration Example	<b>5-8</b>
<i>Figure 5-5</i>	Ethernet Interface Configuration Example	<b>5-9</b>
<i>Figure 5-6</i>	RIP Configuration Example	<b>5-10</b>
<i>Figure 5-7</i>	Routing Table Configuration Example	<b>5-11</b>
<i>Figure 5-8</i>	Adding a Route Example	<b>5-11</b>
<i>Figure 5-9</i>	Syslog Configuration Example	<b>5-12</b>
<i>Figure 5-10</i>	Access List Configuration Example	<b>5-13</b>
<i>Figure 5-11</i>	Add Access List Entry Example	<b>5-14</b>
<i>Figure 5-12</i>	Subsystem Access Configuration Example	<b>5-15</b>
<i>Figure 5-13</i>	Device Reloading Example	<b>5-16</b>
<i>Figure 5-14</i>	Save Changes Button	<b>5-16</b>
<i>Figure 5-15</i>	Change Password Example	<b>5-17</b>
<i>Figure 5-16</i>	SNMP Configuration Example	<b>5-18</b>
<i>Figure 5-17</i>	SNMP Trap Example	<b>5-19</b>
<i>Figure 5-18</i>	Add SNMP Trap Host Example	<b>5-20</b>
<i>Figure 5-19</i>	Private Keys Tab	<b>5-21</b>
<i>Figure 5-20</i>	Add Private Key Example	<b>5-22</b>

<i>Figure 5-21</i>	Importing a Private Key File Example	<b>5-23</b>
<i>Figure 5-22</i>	Certificates Tab	<b>5-24</b>
<i>Figure 5-23</i>	Add Certificate Example	<b>5-25</b>
<i>Figure 5-24</i>	Importing a Certificate Example	<b>5-26</b>
<i>Figure 5-25</i>	Security Policies Tab	<b>5-27</b>
<i>Figure 5-26</i>	Add Security Policy Example	<b>5-28</b>
<i>Figure 5-27</i>	Secure Servers Tab	<b>5-29</b>
<i>Figure 5-28</i>	Add Secure Server Information Example	<b>5-30</b>
<i>Figure 5-29</i>	Server Certificate and Security Policy Example	<b>5-31</b>
<i>Figure 5-30</i>	Add Secure Server Information Example	<b>5-31</b>
<i>Figure 5-31</i>	Add URL Rewrite Rule Example	<b>5-32</b>
<i>Figure 5-32</i>	Certificate Groups Tab	<b>5-33</b>
<i>Figure 5-33</i>	Add Certificate Group Example	<b>5-34</b>
<i>Figure 5-34</i>	Assign Certificate Group Example	<b>5-35</b>
<i>Figure 5-35</i>	Configuring for Other Protocols Example	<b>5-36</b>
<i>Figure 5-36</i>	Generating a Private Key	<b>5-37</b>
<i>Figure 5-37</i>	Key Not Displayed Example	<b>5-38</b>
<i>Figure 5-38</i>	Key Displayed Example	<b>5-39</b>
<i>Figure 5-39</i>	Generate CSR Example	<b>5-40</b>
<i>Figure 5-40</i>	Generate Self-Signed Certificate	<b>5-41</b>
<i>Figure 5-41</i>	Self-Signed Certificate Example	<b>5-42</b>
<i>Figure 5-42</i>	Successfully Generated Self-Signed Certificate	<b>5-43</b>
<i>Figure 5-43</i>	Import PKCS#7 Certificate Group Example	<b>5-44</b>
<i>Figure 5-44</i>	Import PKCS#12 Certificate Group Example	<b>5-45</b>
<i>Figure 5-45</i>	Starting the Secure Server Wizard	<b>5-46</b>
<i>Figure B-1</i>	Single Secure Content Accelerator Installation	<b>B-2</b>
<i>Figure B-2</i>	Secure Content Accelerator Installation with a Load Balancer	<b>B-3</b>



<i>Figure B-3</i>	Secure Content Accelerator In-Line Installation	<b>B-5</b>
<i>Figure B-4</i>	Secure Content Accelerator Transparent Sandwich Installation	<b>B-8</b>
<i>Figure B-5</i>	Secure Content Accelerator One-Armed Non-Transparent Proxy Installation	<b>B-17</b>
<i>Figure B-6</i>	Secure Content Accelerator One-Armed Transparent Proxy Installation	<b>B-23</b>
<i>Figure C-1</i>	Command Hierarchy	<b>C-5</b>
<i>Figure D-1</i>	Troubleshooting Flowchart 1	<b>D-5</b>
<i>Figure D-2</i>	Troubleshooting Flowchart 2	<b>D-6</b>
<i>Figure D-3</i>	Troubleshooting Flowchart 3	<b>D-7</b>
<i>Figure E-1</i>	Port Blocking	<b>E-3</b>
<i>Figure E-2</i>	Port Blocking with Dropped Traffic	<b>E-3</b>





## TABLES

<i>Table 1-1</i>	Secure Content Accelerator Model Differences	<b>1-3</b>
<i>Table 2-1</i>	Secure Content Accelerator LED Descriptions	<b>2-6</b>
<i>Table 6-1</i>	Commands Unavailable in FIPS Mode	<b>6-7</b>
<i>Table 6-2</i>	FIPS Mode Command Changes	<b>6-8</b>
<i>Table A-1</i>	AC Electrical Specifications	<b>A-2</b>
<i>Table A-2</i>	Environmental Specifications	<b>A-2</b>
<i>Table A-3</i>	Physical Specifications	<b>A-3</b>
<i>Table B-1</i>	In-Line Installation Device Configuration	<b>B-6</b>
<i>Table B-2</i>	Transparent Sandwich Installation Device Configuration	<b>B-10</b>
<i>Table B-3</i>	One-Armed Non-Transparent Proxy Installation Device Configuration	<b>B-18</b>
<i>Table B-4</i>	One-Armed Transparent Proxy Installation Device Configuration	<b>B-25</b>
<i>Table C-1</i>	Input Data Formats	<b>C-2</b>
<i>Table C-2</i>	Key Reference	<b>C-3</b>
<i>Table C-3</i>	Output Description for show ssl errors	<b>C-44</b>
<i>Table C-4</i>	Abbreviations Used for show ssl errors continuous	<b>C-48</b>
<i>Table C-5</i>	Output Description for show ssl statistics	<b>C-53</b>
<i>Table C-6</i>	Abbreviations Used for show ssl statistics continuous	<b>C-54</b>
<i>Table D-1</i>	Troubleshooting the Hardware	<b>D-2</b>
<i>Table E-1</i>	Secure Content Accelerator Cryptographic Algorithms	<b>E-11</b>
<i>Table F-1</i>	Regulatory Standards Compliance	<b>16</b>





## About This Guide

---

This guide can help you successfully install and configure the Cisco 11000 Series Secure Content Accelerators (SCA and SCA2). It also provides helpful troubleshooting suggestions for potential hardware and software problems.

## How to Use This Guide

This section describes the contents of this guide.

Section	Description
Chapter 1, Overview	This chapter describes the features and functions of the Secure Content Accelerator.
Chapter 2, Installing the Hardware and Software	This chapter describes how to install the Secure Content Accelerator as a free-standing or rack-mount unit.
Chapter 3, Using the QuickStart Wizard	This chapter provides instructions for using the QuickStart wizard.
Chapter 4, Using the Configuration Manager	This chapter describes how to use the configuration manager to configure the SSL appliance.

Section	Description
Chapter 5, Graphical User Interface Reference	This chapter describes how to use the Graphical User Interface (GUI) to configure the Cisco Secure Content Accelerator. The GUI provides a convenient, web browser-based method of configuring SSL appliances.
Chapter 6, FIPS Operation	This chapter provides a basic introduction to FIPS and describes how to configure the Secure Content Accelerator for FIPS operation.
Appendix A, Specifications	This appendix provides specifications for the Secure Content Accelerator.
Appendix B, Deployment Examples	This appendix provides examples for configuring and deploying the Secure Content Accelerator in conjunction with other networking hardware.
Appendix C, Command Summary	This appendix provides detailed command descriptions and examples to help you take advantage of Secure Content Accelerator features.
Appendix D, Troubleshooting	This appendix provides information to help you isolate and solve problems. It also provides information on using the Cisco Connection Online.
Appendix E, SSL Introduction	This appendix presents a short introduction to SSL and a description of how the components are used in configuration. Instructions for generating keys and certificates with OpenSSL is also included chapter.
Appendix F, Regulatory Information	This appendix provides information on regulatory compliance.

Section	Description
Glossary	This section provides definitions of terms used in this document.
Index	The index provides a detailed list to help you locate specific information quickly.

## Symbols and Conventions

This guide uses the following symbols and conventions to emphasize certain information.



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before you connect the system to its power source.



Caution

A caution means that a specific action you take could cause a loss of data or adversely impact use of the equipment.



Note

A note provides important related information, reminders, and recommendations.

**Bold text** indicates a command in a paragraph.

*Courier text* indicates text that appears in a command line (such as the command line interface) or is returned by the computer.

***Courier bold text*** indicates commands and text you enter in a command line.

*Italic text* indicates the first occurrence of a new term, book title, and emphasized text.

1. A numbered list indicates that the order of the list items is important.
  - a. An alphabetical list indicates that the order of the secondary list items is important.
- A bulleted list indicates that the order of the list topics is unimportant.
  - An indented dashed list indicates that the order of the list topics is unimportant.

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.



## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products Marketplace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.



# Overview

---

This chapter describes the features and functions of the Secure Content Accelerator. This chapter contains the following sections:

- Product Overview
- Secure Content Accelerator Versions
- Released Platforms

# Product Overview

The Secure Content Accelerator is a Secure Sockets Layer (SSL) offloading solution, allowing servers to provide both secure and non-secure services at the same high speeds. You can secure a server for testing purposes immediately using a pre-loaded default key and certificate rather than wait up to a week for your key and certificate to arrive. Simply load your own certificate and key when they are available.

The Cisco 11000 Series Secure Content Accelerator is compatible with all Cisco content switches—the Cisco LocalDirector, the Catalyst Content Switching Module, and the Cisco CSS 11000 Series Content Services Switches.

The Secure Content Accelerator provides:

- Secure URL rewrite, preventing URL redirects and references from breaking or circumventing SSL sessions.
- FIPS-compliant operation
- Firmware signatures are verified during startup and when a firmware image is uploaded to or loaded on the device.
- Compliance with the IEEE 802.3u standard
- Management via command line and Web-based graphical user interfaces
- Encrypted management session option
- User-selectable management UDP/TCP service port option
- RIP client version 1 and 2 support
- Multiple SNTP server support
- SNMP MIB-II support (read-only)
- Transparent/non-transparent SSL proxy toggling
- Non-SSL traffic blocking when operating in default in-line (dual-port) mode
- Arbitrary certificate size
- Netscape International Step-Up Certificate and Microsoft Server Gated Cryptography support
- Private key security
- Client and server certificate authentication
- On-device key and certificate generation

- HTTPS, IMAPS, POP3S, NNTPS, and LDAPS as well as TLS version 1.0, and SSL version 2.0 and 3.0 support

## Secure Content Accelerator Versions

This document applies to all Secure Content Accelerator hardware models, the SCA and SCA2. Any differences in displayed information are described where applicable. The table below presents the differences between the two Secure Content Accelerator models.

*Table 1-1 Secure Content Accelerator Model Differences*

Feature	SCA	SCA2
Maximum Connections	5000	30,000
Maximum Session Cache	75,000	300,000
Maximum SSL Servers	255	4095
Maximum Keys	255	4095
Maximum Certificates	255	4095
CPU	250 MHz Motorola 8240	600 MHz IBM 750CXE
RAM	64MB	256MB
Flash	16MB	32MB
Cryptographic Engine	Rainbow FastMap 200	Broadcom 5821
Maximum 1024-bit RSA Operations/Second	200	4000
Hardware Digest	No	Yes
Hardware Cipher	No	Yes
Hardware RNG	No	Yes

# Released Platforms

The remote configuration manager supports Linux Red Hat versions 5.2, 6.0, 6.1, 6.2, and 7.0; Windows NT 4.0; Windows 2000; and Solaris 2.6, 7, and 8 operating systems. The CD-ROM subdirectory entitled **Docs** contains Adobe Acrobat .pdf versions of the product documentation and release notes.





# Installing the Hardware and Software

---

This chapter describes how to install the Secure Content Accelerator as a free-standing or rack-mounted unit. Suggestions for using the Secure Content Accelerator in conjunction with other networking hardware are described in Appendix B , Deployment Examples.

This chapter contains the following sections:

- Site Requirements
- Shipment Contents
- Unpacking the Secure Content Accelerator
- Installing the Hardware
- Panel Descriptions
- Connecting to Power
- Connecting to Ethernet
- Installing the Software

# Site Requirements

Before you select an installation site for the Secure Content Accelerator, read the electrical, environmental, and physical requirements as described in Appendix A.



Warning

---

**Before you install, operate, or service the system, read the Site Preparation and Safety Guide. This guide contains important safety information you should know before working with the system. Please see Appendix A.**

---

## Required Tools and Equipment

To install the Secure Content Accelerator, you need the following tools and equipment:

- A Phillips screwdriver
- Rack-mount screws and appropriate screwdriver

## Shipment Contents

The Secure Content Accelerator shipment contains the following items:

- Secure Content Accelerator
- Mounting brackets and hardware
- Null modem cable
- Two power cables
- Secure Content Accelerator Documentation
- Secure Content Accelerator compact disk containing:
  - Release Notes
  - Configuration Software
  - PDF version of this guide
  - Firmware files

# Unpacking the Secure Content Accelerator

The Secure Content Accelerator is shipped in a protective carton. The appliance is a self-contained chassis; no modules or components can be added or removed.



## Note

---

A tamper-evident sticker is affixed to the Secure Content Accelerator. When using the device for FIPS-compliant operation, this sticker must remain in place and untouched.

---

To unpack the Secure Content Accelerator:

1. Remove all enclosed packing materials. Save the packing materials in case you need to repack the Secure Content Accelerator later.
2. Remove all accessories from the shipping carton.
3. Check the accessories against the items listed in the section “Shipment Contents”.

# Installing the Hardware



## Warning

---

**Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord. This unit has more than one power cord. To reduce the risk of electric shock, disconnect the two power supply cords before servicing the unit. The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

---

The Secure Content Accelerator can be placed on a flat surface as a free-standing unit or rack-mounted in an equipment cabinet. The following sections describe the steps to install the Secure Content Accelerator as a:

- Free-standing unit
- Rack-mounted unit

Prior to installing the Secure Content Accelerator, observe the following installation requirements:

- The Maximum Rated Ambient Temperature (Tmra) for the Secure Content Accelerator is 105° F (40° C). To ensure the Tmra for this device is not exceeded, allow at least 1 inch (2.54 cm) of space around the four sides of the Secure Content Accelerator.
- This equipment is designed to support only its own weight. Do not place other equipment or material on the Secure Content Accelerator.

**Warning**

---

**Review nameplate ratings for correct voltage and load requirements. For safety, this equipment is required to be grounded through the ground conductor of the AC power cords. Do not remove the cover of the Secure Content Accelerator. There are electrical shock hazards present in the unit if the cover is removed. To reduce the risk of fire or electric shock, do not expose the Secure Content Accelerator to rain or moisture. To disconnect power, remove both power cords. Please review the caution label on the Secure Content Accelerator.**

---

## Installing as a Free-Standing Unit

Position the Secure Content Accelerator on a level surface in an area with access to your network cabling. When installing the Secure Content Accelerator note that Ethernet and serial cables attach to the front of the chassis and power cables attach to the back.

## Installing as a Rack-Mounted Unit



### Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: 1) This unit should be mounted at the bottom of the rack if it is the only unit in the rack. 2) When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. 3) If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Before you begin, you will need the mounting brackets and six screws shipped with the Secure Content Accelerator, a #2 Phillips screwdriver, rack-mounting screws and an appropriate screwdriver.

1. Position the Secure Content Accelerator with the front panel facing you.
2. Position a mounting bracket on one side of the chassis, aligning the holes in the bracket with the screw holes on the chassis.
3. Secure the bracket to the chassis with three screws and the Phillips screwdriver.
4. Repeat steps 2 and 3 to install a mounting bracket on the other side of the chassis.
5. Raise the Secure Content Accelerator to the installation height. Align the screw holes of the mounting brackets with the holes on the equipment rack.
6. Use the appropriate screwdriver and screws to secure each mounting bracket to each side of the rack.

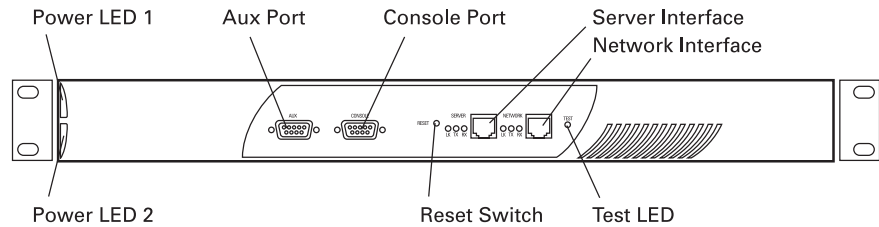
## Panel Descriptions

The front panel of the Secure Content Accelerator, shown in Figure 2-1, contains the following connectors, switches, and LEDs:

- Two DB9 serial ports, marked “AUX” and “CONSOLE”
- Two RJ-45 10/100 Ethernet interface ports, marked “SERVER” and “NETWORK”

- Three Ethernet management LEDs associated with each port
- One “TEST” LED
- One “RESET” switch

**Figure 2-1 Secure Content Accelerator Front Panel**



The rear panel of the Secure Content Accelerator, shown in Figure 2-2, contains the following connectors and switches:

- Two power inputs
- Two power switches

**Figure 2-2 Secure Content Accelerator Rear Panel**

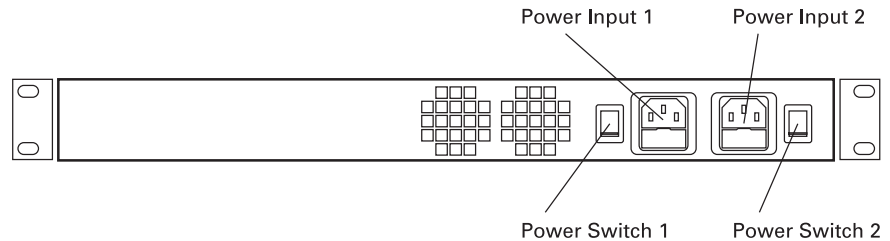


Table 2-1 describes the functional LEDs on the Secure Content Accelerator.

**Table 2-1 Secure Content Accelerator LED Descriptions**

LED Name	Color	State	SCA	SCA2
LK	Green	Off	No link established	N/A
		On	Link established	N/A

**Table 2-1 Secure Content Accelerator LED Descriptions**

LED Name	Color	State	SCA	SCA2
LNK	Green	Off	N/A	No link established
		On	N/A	Link established
TX	Amber	Blinking	Transmit activity detected	N/A
ACT	Amber	Blinking	N/A	Transmit activity detected
RX	Green	Blinking	Receive activity detected	N/A
100	Green	Off	N/A	10Mbps
		On	N/A	100Mbps
Power	White	Off	Power supply is not working	
		On	Power supply is working	
Test	Amber	Off	Self-diagnostics are successful	
		On	Self-diagnostics are running	

## Identifying SCA Models

SCA and SCA2 models can be differentiated by the text on the product label.

## Connecting to Power

The Secure Content Accelerator is powered by dual AC power supplies. Before you install the power cords, ensure that you have read Appendix A for electrical specifications.

1. Ensure that the Secure Content Accelerator power switches are in the **0** (off) position.
2. Attach the power cables to the Secure Content Accelerator by plugging the AC power cord connector into the power receptacle at the rear panel.
3. Plug the power cords into dedicated three-wire grounding receptacles.

4. Switch the power switches to the **1** (on) position.

**Note**

---

Connect the power supplies to different circuits to further ensure appliance availability.

---



# Connecting to Ethernet

This section describes how to attach the Secure Content Accelerator to Ethernet. For network deployment instructions and suggestions, see Appendix B, Deployment Examples.



## Caution

---

If you are using the Secure Content Accelerator in two-port mode, you must connect the cables to it so that client requests (inbound) and server requests (outbound) move through different ports. Inbound traffic uses the “Network” port; outbound traffic uses the “Server” port. If you are using the appliance in one-port mode, you must connect it so that both client requests and server traffic travel through the “Network” port. Use only Category 5 UTP cables with RJ-45 connectors. The Secure Content Accelerator Ethernet interfaces are configured as NIC ports. Use a *straight-through* cable to connect the Secure Content Accelerator to a hub or switch. Use a *crossover* cable to connect the Secure Content Accelerator to a NIC.

---

1. Connect the “Network” port to the Internet.
2. Connect the “Server” port to the servers (or to the “Network” port if using one-port mode).
3. Check the LK LEDs for connection viability. If one or both LK LEDs are not lit, see Appendix D, Troubleshooting, for suggestions.

# Installing the Software

A version of the configuration utility is stored on the SSL appliance. You may use a serial or Telnet connection, or a Web browser to use the device-stored version for configuration. To install the remote configuration manager, follow the appropriate instructions below.



## Note

---

Certain functions are not available in all configuration methods. See Appendix C for more information.

---

**Note**


---

When using the device in FIPS-compliant operation, only a serial management connection is allowed.

---

## Linux Software

You must be logged into the system as a root user before installing the software.

1. Insert the CD-ROM into the computer CD-ROM drive.
2. Enter the following commands:

```
mount -o map=off /mnt/cdrom
cd /mnt/cdrom/Linux/i386
./install_csca
```

To run the configuration manager, enter **csacfg** at a Linux shell prompt.

## Solaris Software

You must be logged into the system as a root user before installing the software.

1. Insert the CD-ROM into the computer CD-ROM drive.
2. Enter the following command:
3. Respond to the following screen prompt, pressing **Enter** to install the software:

```
The following packages are available:
```

```
1. CSCAconfig      Cisco Configuration Manager
```

```
Select package(s) you wish to process (or "all" to process all
packages). (default: all) [?,?,q]
```

4. Type **q** to exit after installation.

To run the configuration manager, enter **csacfg** at a Unix shell prompt.

## Windows NT and Windows 2000 Software

1. Insert the CD-ROM into the computer CD-ROM drive.
2. Double-click the **My Computer** icon to open it.
3. Double-click the CD icon.
4. Double-click the **MSWin** icon to open the directory.
5. Double-click the **WinNT4** icon (Windows NT) or **Win2K** icon (Windows 2000) to open the directory.
6. Double-click the **setup.exe** application to run it. An Install Shield application opens. Follow the instructions on the screen to install the configuration manager and OpenSSL.

To start the configuration manager, use the **Start** menu and point to **Programs>Cisco Systems> Cisco Secure Content Acc. Manager**, or double-click the shortcut on the desktop.





## Using the QuickStart Wizard

---

The QuickStart wizard helps you set up the SSL appliance rapidly using the most basic information. To perform a more advanced configuration, use the configuration manager as described in Chapter 4. The QuickStart wizard presented in this chapter is available only from a CLI-based management session. See Chapter 5 for information about using the Secure Server wizard from a GUI-based management session.

This chapter contains the following sections:

- Before You Begin
- Initiating a Management Session
- Starting the QuickStart Wizard
- Using the QuickStart Wizard
- Using the QuickStart Wizard with a Configured Appliance

## Before You Begin

Before configuring the SSL appliance you must have a certificate and keys for the server. You can use the files you received from the Certificate Authority, copy the keys and certificate from an existing secure server, use default keys and certificates preloaded in the device, or generate your own keys and certificates.

Instructions for exporting keys and certificates from existing server are found in “Using Existing Keys and Certificates” in Appendix E.

Additionally, be aware that you might have to make several changes to your Web pages. The nature of the changes depends upon whether you are securing a previously unsecured site, or adding the SSL appliance to an already secure server installation. These changes are described in the section “Web Site Changes” in Appendix B, Deployment Examples.

**Note**

---

When using the QuickStart wizard in FIPS Mode, only FIPS-approved algorithms are available.

---

## Initiating a Management Session

Use the appropriate instructions below to initiate a management session with the Cisco Secure Content Accelerator.

**Note**

---

When using the Secure Content Accelerator in FIPS Mode, only serial management is allowed.

---

## Serial Management and IP Address Assignment

Follow these steps to initiate a management session via a serial connection and set an IP address for the device.

**Note**

---

When configuring an SCA2 via a serial connection, the displayed prompt is “SCA2” unless a hostname has been defined for the device.

---

**Note**

---

The default terminal settings on the SSL devices and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, please use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

---

1. Attach the included null modem cable to the appliance port marked “CONSOLE”. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings: 9,600 baud, 8 data bits, no parity, 1 stop bit, no flow control.
3. Press **Return**. Initial information is displayed followed by an `SCA>` prompt.
4. Enter Privileged and Configuration modes and set the IP address using the following commands. Replace the IP address in the example with the appropriate one.

```
SCA> enable
SCA# configure
(config[SCA])# ip address 10.1.2.5 netmask 255.255.255.0
(config[SCA])#
```

**Note**

---

When prompted to supply a file name during serial management, you must supply it as a URL in the form of `HOST/PATH/FILENAME` using the `http://`, `https://`, `ftp://`, or `tftp://` prefix.

---

## Telnet

After you have assigned an IP address to the Cisco Secure Content Accelerator using the serial connection or remote configuration manager, you can connect to the appliance via telnet.

1. Initiate a telnet session with the IP address previously assigned to the appliance.
2. An `SCA>` prompt is displayed.

**Note**

---

When prompted to supply a file name during a telnet management session, you must supply it as a URL in the form of HOST/PATH/FILENAME using the http://, https://, ftp://, or tftp:// prefix.

---

## Remote Configuration Manager Application

Use the appropriate instructions below to run the CLI configuration manager.

### Linux

Enter **csacfg** at a Linux shell prompt.

### Solaris

Enter **csacfg** at a Unix shell prompt.

### Windows NT and Windows 2000 Software

To start the configuration manager, use the **Start** menu and point to **Programs>Cisco Systems** and click **Cisco Secure Content Acc. Manager**, or double-click the shortcut on the desktop.



# Starting the QuickStart Wizard

Follow the instructions below appropriate to the management session initiated.

## Using a Serial or Telnet Connection

After initiating a management session as described previously, start the QuickStart wizard via a serial or telnet connection by entering these commands:

```
enable
quick-start
```

If you are using telnet, go to “Using the QuickStart Wizard” below.

If you are using a serial connection and the device has not been assigned an IP address, you are prompted to assign a hostname and IP address before beginning the QuickStart configuration process.

```
Would you like to specify a hostname and IP address for this device?:
```

```
Enter the hostname for this device:
```

The hostname is a user-specified device name. In this example, we use the name *myDevice*. When prompted for them, enter the IP address, netmask, and default gateway for the device. You are prompted to accept the information before continuing with configuration.

The following configuration will be saved to the device.

```
Hostname                : myDevice
Ip address              : 10.1.11.100
Netmask                 : 255.255.255.0
Default gateway addr    : 10.1.11.10
```

```
Is the above information correct? (y/n):
```

Enter **y** if the listing is correct. Go to “Using the QuickStart Wizard” below. Enter **n** if the information is incorrect. You are prompted for the configuration information again.

## Using the Remote Configuration Manager

Run the configuration manager as described previously. Enter the command **show device list** to list all Cisco Secure Content Accelerator devices detected by the configuring computer.



### Note

---

When the appliance is configured in the default two-port mode, the configuring computer must be connected via the “Server” port. If the appliance is configured to use one-port mode, the configuring computer must be connected via the “Network” port.

---

If only the new device is listed, attach the configuration manager and enter Privileged mode using the following command sequence, entering the appropriate IP address and netmask when prompted:

#### **attach**

*CS-macaddress* must be assigned an ip address before attaching.

Enter an IP address for *CS-macaddress*:

Enter the netmask for *CS-macaddress* (*suggested netmask*):

If more than one device is listed, attach the configuration manager and enter Privileged mode by using the following command sequence, entering the appropriate IP address and netmask when prompted:

#### **on CS-macaddress attach**

*CS-macaddress* must be assigned an ip address before attaching.

Enter an IP address for *CS-macaddress*:

Enter the netmask for *CS-macaddress* (*suggested netmask*):

In either case, *macaddress* is the hyphen-delimited MAC address of the device. A netmask is suggested. The following prompt appears.

Would you like to use the QuickStart wizard for *CS-ipaddress*? (y/n):

(The IP address is the same as the one you assigned to the device.) Type **y** to continue with the QuickStart wizard. Typing **n** launches the configuration manager. Go to “Using the QuickStart Wizard”.

# Using the QuickStart Wizard

**Note**

---

Screen text displayed in this section reflects that found in the QuickStart wizard for the remote configuration manager. Information for appropriate responses through all configuration manager methods is presented.

---

Read the opening screen information and respond to the prompt.

```
Would you like to use the QuickStart wizard to create an ssl-server?  
(y/n):
```

If you do not have a key and certificate available and do not wish to use a default key and certificate, enter **n** or **q**. If you have read and agree with the introductory information, enter **y**. The following text is displayed:

```
Enter a name for your ssl-server:
```

Enter a name for the logical secure server (“ssl-server”) you are configuring. The name is used for identification purposes only. (In this example, we name the server *myServer*.) If it already exists, you are asked to provide a different name.

**Note**

---

Secure server names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Secure server names must begin with an alphabetic character and have a limit of 15 characters.

---

```
Enter the IP address for 'myServer':
```

This is the IP address of the real server to which the clear text should be sent.

```
Enter the SSL port [443]:
```

Enter the TCP service port for the appliance to monitor for secure connection requests. The default is 443, but you can specify a different number. You cannot specify a TCP service port already configured to the same IP address.

Enter the clear text port:

Enter the number of the TCP service port for the SSL appliance to use to send clear text to the server. If you specify TCP service port 80, you are warned that the port will be unavailable for non-SSL requests. (See Chapter 3 for a discussion of port blocking.) You can abort the current clear text port designation and enter a different TCP service port, or approve using TCP service port 80 for clear text.

You have completed TCP service port configuration of the logical secure server and are ready to specify a key to use.

```
CONFIGURE SSL-SERVER 'myServer' KEY
```

```
SSL-server name   : myServer
Ip address        : 10.1.2.3
Secure Port       : 443
Clear Port        : 80
```

Each ssl-server is associated with a key.

1. Key is stored in a file on a disk.
2. Want to use an existing or default Key.

Choose the option corresponding to your situation (1/2):



#### Note

---

If you are using a key created with an IIS or non-PEM-encoded key or certificate, use the default keys and certificates included with SSL device. After configuring the device with the QuickStart wizard, use the configuration manager to load your own certificate and key. See “Example: Setting up a Secure Server” in Chapter 4 and “SSL Configuration Command Set” in Appendix C.

---

If you have the *key on disk or available via a URL*, type **1**.

Enter the name of the key for ssl-server 'myServer':

Enter the name to assign a key. This name is used for identification only.

**Note**

Key names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Key names must begin with an alphabetic character and have a limit of 15 characters.

Enter PEM encoded X509 private key filename:

Enter the file name and path or the URL for the key as prompted. If the QuickStart wizard is unable to find or load the file, you receive an error message and are allowed to restart key assignment. After the key is properly loaded, configure the certificate as described below.

To use a *key already loaded into the appliance* (including defaults) rather than key on disk, type **2** when prompted to choose an option. All available keys are displayed. Enter the name of the key to use. If you enter an invalid key name, you receive an error message and are prompted to re-enter the key name.

After the key has been properly loaded, you are shown a summary and asked to configure a certificate.

```
CONFIGURE SSL-SERVER 'myServer' CERTIFICATE
```

```
SSL-server name      : myServer
Ip address           : 10.1.2.3
Secure Port         : 443
Clear Port           : 80
Key name             : default
```

Each ssl-server is associated with a certificate.

1. Certificate is stored in a file on a disk.
2. Want to use an existing or default Certificate.

Choose the option corresponding to your situation (1/2):

If you have the *certificate on disk or available via a URL*, type **1**.

Enter the name of the certificate for ssl-server 'myServer':

Enter the name to assign the certificate. This name is used for identification only.

**Note**

---

Certificate names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Certificate names must begin with an alphabetic or underscore character and have a limit of 127 characters.

---

Enter PEM encoded X509 private certificate filename:

Enter the file name and path or URL for the certificate as prompted. If the QuickStart wizard is unable to find or load the file, you receive an error message and are allowed to restart certificate assignment. After the certificate is properly loaded, configure a security policy as described below.

To use a *certificate already loaded into the appliance* (including default certificates) rather than certificate on disk, type **2** when prompted to choose an option. All available certificates are displayed. Enter the name of the certificate to use. If you enter an invalid certificate name, you receive an error message and are prompted to re-enter the certificate name.

**Note**

---

When using default keys and certificates, the certificate and key you choose must match. The pre-loaded “Default” and “Default-512” keys and certificates are interchangeable and can be used in combination. The “Default-1024” key and certificate must be used in conjunction. If you have entered a key and certificate that cannot be used together, you are asked whether to re-enter the key and certificate. If you do not choose to re-enter the key and certificate, your choices are accepted, but the secure server is not configured correctly and will not function properly.

---

After the certificate has been properly loaded, you are shown a summary and asked to specify a security policy.

```
CONFIGURE SSL-SERVER 'myServer' SECURITY POLICY
```

```
SSL-server name      :myServer
IP address           :10.1.2.3
Secure Port          :443
Clear Port           :80
Key name             :default
Cert name            :default
```

You need to enter a security policy for ssl-server 'myServer'. To simplify the encryption algorithms, you have 3 options:

```
strong - RSA key size of 1024, DES_SHA1, 3DES_SHA1, ARC4_MD5 and
ARC4_SHA1
weak - RSA key size of 512, exp DES_SHA1, ARC2_MD5, ARC4_MD5 and
ARC4_SHA1
default- RSA key size of 1024, ARC4_MD5, ARC4_SHA1 and exp
ARC4_MD5, ARC4_SHA1, MD5
```

ARC4 is compatible with RC4™ RSA Data Security; ARC2 is compatible with RC2™ RSA Data Security.

Enter the security policy for ssl-server 'myServer' [default]:

At the prompt, enter the name of the security policy to use. The “strong” policy includes the most secure algorithms. The “weak” policy algorithms are less secure and appropriate for export use. The “default” policy algorithms are those most commonly used. See Chapter 3 for more algorithm information. If you enter an invalid security policy name, you receive an error message and are prompted to re-enter the name.



#### Note

---

When using the QuickStart wizard in FIPS Mode, only the FIPS security policy is available. The FIPS security policy contains only FIPS-approved algorithms.

---

After the name of the security policy is accepted, you are prompted to verify the logical secure server configuration.

```
SSL-SERVER 'myServer' SUMMARY
```

The following SSL-server will be created:

```
SSL-server name      :myServer
IP address           :10.1.2.3
Secure Port          :443
Clear Port           :80
Key name              :default
Cert name             :default
Security Policy name :strong
```

Is the above information correct? (y/n) :

If the information is correct, type **y**. The logical secure server you have configured is created. If you type **n**, the server configuration process restarts using the current secure server.

Would you like to use the QuickStart wizard to create another ssl-server? (y/n):

Type **y** to begin the server configuration process again with a new server. Type **n** to set a configuration (enable) password for the device.

```
SETUP CONFIGURATION PASSWORD PROTECTION
```

Would you like to set a password to protect configuration of the SSL-R? (y/n):

Type **y**, and enter a password. Re-enter it to confirm.

You must set an enable password for the device to ensure its configuration security. The password you enter is not displayed.

Would you like to set a name for this device? (y/n/q):

Type **y**, and enter a name for the SSL appliance.

A default gateway is needed to connect outside of your local subnet.

Would you like to set a default gateway for this device? (y/n/q): **y**  
Enter a default gateway for this device:

A default gateway is needed for the device to connect outside of the local subnet. Type **y**, and enter the IP address at the prompt.



A summary screen shows information about the device, keys, certificates, security policies, and the logical secure servers configured on it.

SCA myDevice

#### Keys

Name	Id	RC	V
default	1	0	Y
default-512	2	0	Y
default-1024	3	0	Y

#### Certificates

Name	Id	RCCG	RCPS	V
default	1	0	0	Y
default-512	2	0	1	Y
default-1024	3	0	0	Y

#### Certificate groups

\*no certificate group list entries\*

#### Security Policies

Name	Id	RC	Policy List
default	1	0	ARC4-MD5, ARC4-SHA, EXP-ARC4-MD5, EXP-ARC4-SHA, EXP1024-ARC4-MD5, EXP1024-ARC2-CBC-MD5, EXP1024-ARC4-SHA, NULL-MD5, NULL-SHA
weak	2	0	EXP-ARC4-MD5, EXP-ARC4-SHA, EXP-ARC2-MD5, EXP1024-ARC4-MD5, EXP1024-ARC2-CBC-MD5, EXP1024-DES-CBC-SHA, EXP1024-ARC4-SHA, NULL-MD5, NULL-SHA, EXP-DES-CBC-SHA
fips	3	0	DES-CBC-SHA, DES-CBC3-SHA
strong	4	1	DES-CBC-MD5, DES-CBC-SHA, DES-CBC3-MD5, DES-CBC3-SHA, ARC4-MD5, ARC4-SHA
all	5	0	DES-CBC-MD5, DES-CBC-SHA, DES-CBC3-MD5, DES-CBC3-SHA, ARC4-MD5, ARC4-SHA, EXP-ARC4-MD5, EXP-ARC4-SHA, EXP-ARC2-MD5, EXP1024-ARC4-MD5, EXP1024-ARC2-CBC-MD5, EXP1024-DES-CBC-SHA, EXP1024-ARC4-SHA, NULL-MD5, NULL-SHA, EXP-DES-CBC-SHA
noexport56	6	0	DES-CBC-SHA, DES-CBC3-MD5, DES-CBC3-SHA, ARC4-SHA, EXP-ARC4-MD5, EXP-ARC2-MD5, EXP-DES-CBC-SHA

## SSL Servers

Name	Secure SSL IP	KC	PKey	Secpolicy
Id	Plaintext IP		Cert	CA Group
myServer	10.1.2.3:443	Y	myKey	strong
001	10.1.2.3:80		myCert	

The list of keys includes all those loaded into the device. The columns and their descriptions are shown in the table below.

Column	Description
Id	The number of the key as loaded into the device
RC (Reference Count)	The number of logical secure servers using the key
V (Validity)	The validity of the key as loaded into the device

The list of certificates includes all certificates loaded into the device. The columns and their descriptions are shown in the table below.

Column	Description
Id	The number of the certificate as loaded into the device
RCCG (Reference Count Certificate Group)	The number of certificate groups using the certificate
RCPS (Reference Count Proxy Server)	The number of SSL servers using the certificate
V (Validity)	The validity of the certificate as loaded into the device; “Y” indicates the certificate is valid, “N” indicates the certificate is invalid

The list of security policies includes all those configured on the device. The columns and their descriptions are shown in the table below.

Column	Description
Name	The name of the security policy
Id	The number of the security policy as loaded into the device
RC (Reference Count)	The number of SSL servers using the security policy
PolicyList	The names of the individual cryptographic schemes associated with each security policy

The list of SSL servers includes all those configured on the device. The columns and their descriptions are shown in the table below.

Column	Description
Name	The name of the SSL server
Id	The number of the SSL server as loaded into the device
Secure SSL IP	The IP address and TCP service port to monitor for SSL transaction requests
Plaintext IP	The IP address and TCP service port used to send decrypted SSL traffic to the server
KC	The validity of the key and certificate pair assigned to the SSL server; “U” indicates the key or certificate is not defined, “Y” indicates the key and certificate match, “N” indicates the key and certificate do not match
PKey	The name of the private key assigned to the SSL server
Cert	The name of the certificate assigned to the SSL server
Secpolicy	The name of the security policy assigned to the SSL server
CA Group	The name of the certificate chain, if one has been assigned to the server

You are asked whether to save the configuration to flash memory.

Would you like to save your configuration to flash? (y/n):

If you type **y**, you will be asked to wait while the configuration is saved to flash, and the QuickStart wizard finishes. If you type **n**, the QuickStart wizard finishes.



#### Caution

---

If the configuration is not saved to flash memory, the configuration is lost during a power cycle or when the **reload** command is used.

---

## Using the QuickStart Wizard with a Configured Appliance

If you wish to run the QuickStart wizard for a previously configured Cisco Secure Content Accelerator, follow these steps:

1. Initiate a management session and start the configuration manager as described previously.
2. Use the appropriate method to attach to the device (remote management only), depending upon the number of devices in the list returned by the **show device list** command.
3. Enter Privileged mode.
4. Enter the command **quick-start**. If multiple devices are in Privileged mode when using the remote configuration manager, enter **on devname quick-start**, where *devname* is the name of the device.
5. Go to “Using the QuickStart Wizard”.



#### Note

---

Non-FIPS-compliant servers can be reconfigured with the QuickStart wizard in FIPS Mode using only FIPS 1024-approved SSL security policies.

---



## Using the Configuration Manager

---

This chapter describes how to use the configuration manager to configure the SSL appliance. Refer to Appendix E for a brief introduction to how the Cisco Secure Content Accelerator appliance works with components of the SSL protocol and description of the information you need to begin configuration.

This chapter contains the following sections:

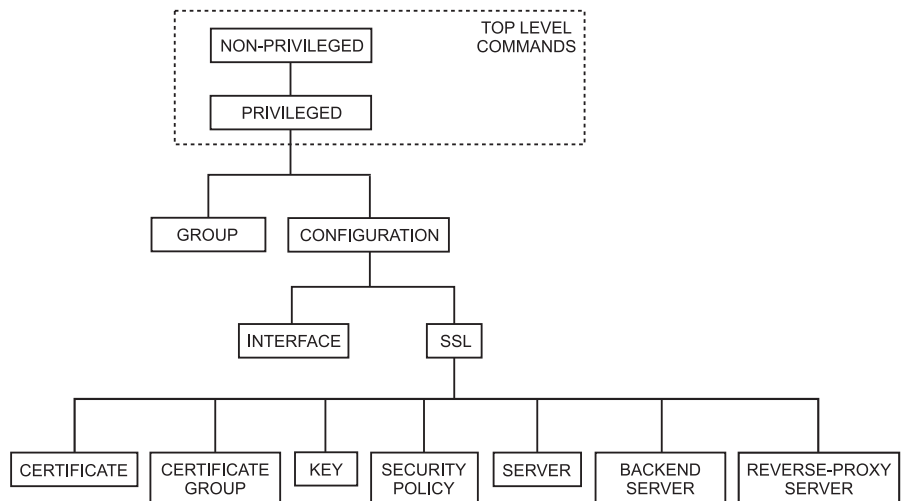
- Overview
- Configuration Security
- Before You Begin
- Initiating a Management Session
- Using the Remote Configuration Manager
- Configuring the Device
- Step-Up Certificates and Server-Gated Cryptography
- Configuring Certificate Groups
- Using Client and Server Certificate Authentication
- Generating Keys and Certificates
- Supporting SNMP
- Supporting RIP
- Supporting Other Secure Protocols

# Overview

Whether used via serial or telnet connection or remotely, the command line interface configuration manager provides greater control over the SSL appliance than the QuickStart or Secure Server wizard alone.

The configuration manager allows you to control hardware and SSL portions of the appliance through a discreet mode and submode system as shown in the hierarchy diagram in Figure 4-1.

**Figure 4-1 Configuration Manager Hierarchy**



To configure items in a submode, activate the submode by entering a command in the mode above it. For example, to set the network interface speed or duplex you must first enter **enable**, **configure**, then **interface network**. To return to the higher Configuration mode, simply enter **end** or **exit** or press **CTRL+D**. The **finished** command returns to the Top Level from any mode. Appendix C lists all commands for SSL devices.



Note

Refer to Chapter 6 for FIPS Mode instructions.

**Note**

---

The system prompts displayed by the configuration manager vary slightly depending upon the management session type used and Secure Content Accelerator version. Secure Content Accelerator version 2 is indicated by an “SCA2” prompt. Unless specifically stated otherwise, all prompts displayed in this chapter reflect those encountered with the remote configuration manager and original SCA version.

---

## Configuration Security

Cisco Secure Content Accelerator devices allow easy, flexible configuration without compromising the security of your network or their own configuration.

## Passwords

Cisco Secure Content Accelerator devices use two levels of password protection: access- and enable-level. *Access-level passwords* control who can attach the remote configuration manager or access the device via telnet and serial connections. *Enable-level passwords* control who can view the same data available with access-level passwords as well as view sensitive data and configure the device.

SSL devices are shipped without passwords. Setting passwords is important because the device can be administered over a network. For more information about passwords, see the commands **password access** and **password enable** in Appendix C.

**Note**

---

FIPS-compliant operation requires both access- and configuration-level passwords. See Chapter 6 for more information.

---

## Access Lists

Access lists control which computers can attach to a specific device. No access lists exist when you first install the Secure Content Accelerator. You can restrict the computers allowed to manage the appliance by adding their IP addresses to one or more access lists for each device. For more information about configuring access lists, see the commands **show access-list**, **access-list**, **snmp access-list**, **remote-management access-list**, **telnet access-list**, and **web-mgmt access-list** in Appendix C.



---

**Note**

In FIPS Mode you can configure access lists but can assign them only to the SNMP subsystem.

---

## Encrypted Management Sessions

To further protect the configuration security, you can specify that remote (non-serial and non-telnet) configuration sessions be encrypted using AES, DES, or ARC4. See **remote-management encryption** in Appendix C.

## Factory Default Reset Password

If you have forgotten your access or enable password, you can use a factory-set password during a serial configuration session. When prompted for a password, enter *FailSafe* (case-sensitive). You are asked to confirm the action. The appliance reboots (reloads) with factory default settings.



---

**Caution**

All configuration is lost when using the factory default reset.

---



## Before You Begin

Before configuring the SSL appliance you must have a certificate and keys for the server. You can use the files you received from the Certificate Authority, copy the keys and certificate from an existing secure server, use default keys and certificates preloaded in the device, or generate your own keys and certificates.

Instructions for exporting keys and certificates from existing server is found in “Using Existing Keys and Certificates” in Appendix E.

Additionally, be aware that you must make several changes to your Web pages. The nature of the changes depends upon whether you are securing a previously unsecured site, or adding the SSL appliance to an already secure server installation. These changes are described in section “Web Site Changes” in Appendix B.

## Initiating a Management Session

Use the appropriate instructions below to initiate a management session with the Secure Content Accelerator.



Note

---

When using the Secure Content Accelerator in FIPS Mode, only serial management is allowed.

---

## Serial Management and IP Address Assignment

Follow these steps to initiate a management session via a serial connection and set an IP address for the device.

**Note**

---

The default terminal settings on the SSL devices and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, please use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

---

1. Attach the included null modem cable to the appliance port marked “CONSOLE”. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings: 9,600 baud, 8 data bits, no parity, 1 stop bit, no flow control.
3. Press **Return**. Initial information is displayed followed by an `SCA>` prompt.
4. Enter Privileged and Configuration modes and set the IP address using the following commands. Replace the IP address in the example with the appropriate one.

```
SCA> enable
SCA# configure
(config[SCA])# ip address 10.1.2.5 netmask 255.255.255.0
(config[SCA])#
```

**Note**

---

When prompted to supply a file name during serial management, you must supply it as a URL in the form of `HOST/PATH/FILENAME` using the `http://`, `https://`, `ftp://`, or `tftp://` prefix.

---

## Telnet

After you have assigned an IP address to the Cisco Secure Content Accelerator using the serial connection or remote configuration manager, you can connect to the appliance via telnet.

1. Initiate a telnet session with the IP address previously assigned to the appliance.
2. An SCA> prompt is displayed.



---

**Note** When prompted to supply a file name during a telnet management session, you must supply it as a URL in the form of HOST/PATH/FILENAME using the http://, https://, ftp://, or tftp:// prefix.

---

## Running the Remote Configuration Manager

Use the appropriate instructions below to run the CLI configuration manager.

### Linux

Enter **csacfg** at a Linux shell prompt.

### Solaris

Enter **csacfg** at a Unix shell prompt.

### Windows NT and Windows 2000 Software

To start the configuration manager, use the **Start** menu and point to **Programs>Cisco Systems** and click **Cisco Secure Content Acc. Manager**, or double-click the shortcut on the desktop.

# Using the Remote Configuration Manager

Enter **show device list** to display a list of all Cisco Secure Content Accelerators in the same broadcast domain as the configuring computer and those found using the discover port command. Devices are listed in the following format:

Type	Key	Name	Version	MacAddr	IPAddr
------	-----	------	---------	---------	--------

Cisco Secure Content Accelerator devices are listed with the “CSS-SCA” device type. Note the MAC address of the device you wish to configure. It is used with the “CS-” prefix to identify a specific device when giving commands in the format *CS-macaddress*, where *macaddress* is the MAC address of the device.



## Note

Identify an unnamed device as a specific appliance, match the last six digits of the serial number with the MAC address shown.

## Specifying Devices

If only one device is listed, you can configure it by simply entering commands as listed. If multiple devices are listed, you must specify the device your commands should address. In these instances you must use the **on** prefix.

For example, entering **show device list** returns the following list of unattached devices:

CSS-SCA	Ru	sslDev1	...
CSS-SCA	Ru	sslDev2	...
CSS-SCA	Ru	sslDev3	...
CSS-SCA2	Ru	sslDev4	...

Secure Content Accelerator version 2 devices are indicated by the type **CSS-SCA2**.

To attach the configuration manager to the device *sslDev3*, enter this command:

```
on sslDev3 attach
```

The auto completer function can assist data entry. See “Editing and Completion Features” in Appendix C for details for using editing and auto completer features.

## Working with Device Groups

The remote configuration manager allows you to create groups of devices for single management sessions. Most Top Level commands can target a group just as they would a single device. Using the device list above, the commands below create a device group named *myGroup*, add three devices, and display the group contents.

```
csacfg> group myGroup create
(group[myGroup])> device sslDev1
(group[myGroup])> device sslDev2
(group[myGroup])> device sslDev4
(group[myGroup])> info
group name: myGroup
number of devices: 3
device: sslDev1
device: sslDev2
device: sslDev4
(group[myGroup])>
```

To remove a device from the group, use the **no** form of the command:

```
(group[myGroup])> no device sslDev2
```

Enter **end** to leave Group configuration mode. To send commands to every device in the group, use the **on** prefix.

```
on myGroup attach
```

You can simplify command entry for this group further by setting the **on** command to address the group *myGroup* by default.

```
set on-prefix myGroup
```

After entering this command, you do not need to use the **on** prefix when addressing the default target. For example, the **on myGroup attach** command becomes **attach**. You can still address another group instead of the default; simply specify its name following the **on** prefix. Change the **on** prefix target by re-entering the command, identifying the new group. View the **on** prefix target by entering **show profile**.



---

**Note** Individual devices can also be set as the **on** prefix default target. Any command without the **on** prefix defaults to the group or device specified by the **set on-prefix** command.

---

For more information about Group Configuration commands, see “Group Configuration Command Set” in Appendix C.

## Remote Configuration Caching

The remote configuration manager caches some management session information. Some changes made during a configuration session may not be displayed. Additionally, configuration changes from multiple concurrent configuration sessions may not be reflected in status and configuration displays. To obtain the most current configuration data, exit the configuration manager, and launch the application again or use the **refresh** command in the Privileged Command set.

## Configuring the Device

When you configure an appliance to perform SSL offloading you are actually setting up one or more logical secure servers whose SSL-related configurations reside in the appliance. Each logical secure server has several attributes:

- A unique IP address for the real server providing content
- Specifications for the appropriate key and certificate to use
- A security policy specifying the cryptographic scheme(s) to use

## Example: Setting up Basic Device Parameters

This example describes how to use the configuration manager to set the basic SSL appliance configuration.



### Note

---

The remote configuration instructions in this example assume only one Cisco Secure Content Accelerator is available for configuration or that you have set the on-prefix to a single device. If you have more than one SSL device available for configuration, refer to section “Specifying Devices” presented previously in this chapter for device identification directions.

---

1. Initiate a serial management session, and set the IP address of the device to 10.1.2.5.

```
SCA> enable
SCA# config
(config[CSS-SCA])# ip address 10.1.2.5 netmask 255.255.0.0
(config[CSS-SCA])#
```

2. If you wish to configure the server using the serial connection, continue with step 3.

If you wish to use a telnet connection, initiate a telnet session with the IP address assigned in step 1, and go to step 3.

If you wish to configure the server using the remote configuration manager, initiate a remote management session, attach to the appliance, and when prompted to use the QuickStart wizard, enter **n**. Go to step 3.



### Note

---

For the remainder of these examples, system prompts are displayed as remote configuration prompts.

---

- Use the following commands to enter Privileged and Configuration modes and change the name of the SSL appliance to *myDevice*.

```
SCA> enable
SCA> configure
(config[CS-10-1-2-3])> hostname myDevice
(config[CS-10-1-2-3])> end
SCA> configure
(config[myDevice])>
```

- Set the default router.

```
(config[myDevice])> ip route default 10.1.2.1
(config[myDevice])>
```

- Set an enable password to protect the appliance configuration. The password is requested whenever the **enable** command is given.




---

**Note** Passwords are not echoed to the screen.

---

```
(config[myDevice])> password enable
Enter new password:
Confirm password:
(config[myDevice])> end
SCA>
```

## Example: Setting up a Secure Server

This example describes how to use the configuration manager rather than the QuickStart wizard to set up a secure server. In this example, the default SSL port (443) and remote port (81) are used.

- Enter Privileged, Configuration, and SSL Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])> ssl
(config-ssl[myDevice])>
```



2. Enter Key Configuration mode and create a key named *myKey*. Load the PEM-encoded key file. Return to SSL Configuration Mode.

```
(config-ssl[myDevice])> key myKey create
(config-ssl-key[myKey])> pem keyFile
(config-ssl-key[myKey])> end
(config-ssl[myDevice])>
```



---

**Note** Use the **der** command when using DER-encoded keys and certificates, the **net-iis** command when using keys exported from IIS 4.

---



---

**Note** Key names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Key names must begin with an alphabetic character and have a limit of 15 characters.

---

3. Enter Certificate Configuration mode and create a certificate named *myCert*. Then load the PEM-encoded certificate file. Return to SSL Configuration Mode.

```
(config-ssl[myDevice])> cert my create
(config-ssl-cert[myCert])> pem certFile
(config-ssl-cert[myCert])> end
(config-ssl[myDevice])>
```



---

**Note** Certificate names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Certificate names must begin with an alphabetic character and have a limit of 127 characters.

---

4. Enter Security Policy Configuration mode and create a security policy named *myPol*. Assign the “strong” cryptography policy to it. Return to SSL Configuration mode.

```
(config-ssl[myDevice])> secpolicy myPol create
(config-ssl-secpolicy[myPol])> crypto strong
(config-ssl-secpolicy[myPol])> end
(config-ssl[myDevice])>
```




---

**Note** When using FIPS Mode only the FIPS security policy is available.

---




---

**Note** Security policy names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Security policy names must begin with an alphabetic character and have a limit of 15 characters.

---

5. Enter Server Configuration mode and create a server named *myServer*. Assign the IP address 10.1.2.4. Assign port 443 for monitoring for SSL connections and port 81 for sending clear text. Assign the key, certificate, and security policies just created. Then exit to Top Level mode.

```
(config-ssl[myDevice])> server myServer create
(config-ssl-server[myServer])> ip address 10.1.2.4
(config-ssl-server[myServer])> sslport 443
(config-ssl-server[myServer])> remoteport 81
(config-ssl-server[myServer])> key myKey
(config-ssl-server[myServer])> cert myCert
(config-ssl-server[myServer])> secpolicy myPol
(config-ssl-server[myServer])> finished
SCA>
```

6. Save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or if the **reload** command when used.

```
SCA> write flash
SCA>
```



---

**Note** You can review the configuration of the currently edited SSL object (key, certificate, certificate chain, security policy, or server) by using the **info** command in the appropriate mode.

---

## Example: Setting up a Backend Server

This example describes how to use the configuration manager to set up a backend server.

1. Enter Privileged, Configuration, and SSL Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])> ssl
(config-ssl[myDevice])>
```

2. Enter Backend Server Configuration mode and create a backend server named *myBackServ*.

```
(config-ssl[myDevice])> backend-server myBackServ create
(config-ssl-backend[myBackServ])>
```

3. Assign an IP address and netmask to the backend server.

```
(config-ssl-backend[myBackServ])> ip address
```

4. Assign port 443 for SSL traffic and port 80 for clear text traffic.

```
(config-ssl-backend[myBackServ])> localport 80
(config-ssl-backend[myBackServ])> remoteport 443
```

5. Specify a security policy for the server.

```
(config-ssl-backend[myBackServ])> secpolicy strong
```



---

**Note** When using FIPS Mode only default security policies and those configured for FIPS 140-2-compliant operation are available.

---

6. Exit to Privileged mode, and save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
(config-ssl-backend[myBackServ])> finished
SCA> write flash
SCA>
```

## Example: Setting up a Reverse-Proxy Server

This example describes how to use the configuration manager to set up a reverse-proxy server.

1. Enter Privileged, Configuration, and SSL Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])> ssl
(config-ssl[myDevice])>
```

2. Enter Reverse-Proxy Server Configuration mode and create a server named *myRevServ*.

```
(config-ssl[myDevice])> reverse-proxy-server myRevServ create
(config-ssl-rproxy[myRevServ])>
```

3. Assign port 8080 for clear text traffic.

```
(config-ssl-rproxy[myRevServ])> localport 8080
```

4. Specify a security policy for the server.

```
(config-ssl-rproxy[myRevServ])> secpolicy strong
```




---

**Note** When using FIPS Mode only default security policies and those configured for FIPS 140-2-compliant operation are available.

---

- Exit to Privileged mode and save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
(config-ssl-rproxy[myRevServ])> finished
SCA> write flash
SCA>
```

**Note**


---

When using this configuration, client browsers must be set to use this device as a proxy.

---

## Example: Configuring Secure URL Rewrite

The Secure URL Rewrite feature prevents URL redirects and references from breaking or circumventing SSL sessions. This example uses the CLI. The same options are available in the GUI.

**Note**


---

The command line in the examples reflects using a serial management session.

---

- Open a management session with the device.
- Enter Privileged, Configuration, and SSL Configuration modes:

```
SCA> enable
SCA# configure
(config[SCA])# ssl
(config-ssl[SCA])#
```

- Enter Server Configuration mode for the server you wish to configure URL rewrites.

```
(config-ssl[SCA])# server myServer
(config-ssl-server[myServer])#
```

- The **urlrewrite** command uses the following syntax:

```
urlrewrite <domainName> [sslport <portid>] [clearport <portid>]
<redirectonly>
```

<i>domainName</i>	The domain or file identifier as a domain name, IP address, or path and file name. An * (asterisk) wild card character can be used to specify more than one server in a single domain, e.g., “*.company.com”.
<b>sslport</b>	Keyword identifying the specified port to be used for SSL traffic.
<i>portid</i>	A port identification for SSL traffic.
<b>clearport</b>	Keyword identifying the specific port to be used for clear text traffic.
<i>portid</i>	A port identification for clear text traffic.
<b>redirectonly</b>	A keyword is used to indicate that only the “Location:” field in the HTTP 30x redirect header should be rewritten. This solves a common problem with Web servers using insecure HTTP 30x redirects.

Enter a URL rewrite rule for the www.mybusiness.com.

```
(config-ssl-server[myServer])# urlrewrite www.mybusiness1.com
sslport 443 clearport 81
```

All references that pass through the device to

http://www.mybusiness1.com:81 are rewritten to

https://www.mybusiness1.com.

To securely rewrite only 30x-series redirects (i.e., 302 or 304) referencing http:// rather than all instances of http:// (such as those that appear intentionally in the application data), use the **redirectonly** option. (This command must be entered on a single line.)

```
(config-ssl-server[myServer])# urlrewrite www.mybusiness2.com
sslport 443 clearport 81 redirectonly
```

5. A wildcard can be used to specify multiple SSL hosts in the same domain.

```
(config-ssl-server[myServer])# urlrewrite *.mybusiness3.com
sslport 443 clearport 81
```



**Note** Do not use \*.com as a filter. The definition is too broad.

Wildcards should be used with care to avoid any unwanted rewriting of references.

- To see the results of these URL rewrite rules in the server configuration, enter the following command. The results are presented below it.

```
(config-ssl-server[myServer])# show ssl server myServer
```

```
...
```

```
URL Rewrite:
```

Name	Clear Port	SSL Port	Redirect Only
www.mybusiness1.com	443	81	No
www.mybusiness2.com	443	81	Yes
*.mybusiness3.com	443	81	No

For more information about URL rewriting, contact your Cisco representative for a copy of the white paper *SSL Offloaders and Contextual Consistency*.

## Example: Configuring SNTP Servers

Up to four SNTP servers can be configured on the Secure Content Accelerator.



### Note

To provide increased security, we recommend using an SNTP server on the internal network. Using an external SNTP server might compromise network security.

- Open a management session with the device.
- Enter Privileged and Configuration modes:

```
SCA> enable
SCA# configure
(config[SCA])#
```

- Enter the IP addresses or host names of up to four SNTP servers. (Host names are resolved to IP addresses in the device configuration.)

```
(config[SCA])# sntp server 10.1.24.2
(config[SCA])# sntp server 10.1.24.4
(config[SCA])# sntp server 10.2.22.2
(config[SCA])# sntp server 10.2.22.6
(config[SCA])#
```

- The default polling interval is 86400 seconds (one day). To change this interval to 43200 seconds (12 hours), enter use the **sntp interval** command.

```
(config[SCA])# sntp interval 43200
(config[SCA])#
```

- To view the results of these commands, you can use either the **show sntp** or **show device** command. The **show sntp** command and an example of returned information are below.

```
(config[SCA])# show sntp
SNTP server sources:
  10.1.24.2    (0/6 fails/tries, stratum 2)
  10.1.24.4    (0/0 fails/tries, stratum 2)
  10.2.22.2    (0/0 fails/tries, stratum 2)
  10.2.22.6    (0/0 fails/tries, stratum 2)
SNTP synchronization interval: 43200 (seconds)
(config[SCA])#
```

The **show device** command and an example of returned information are presented below.

```
(config[SCA])# show device
...
SNTP sync'ing      :   every 43200 (s) from 10.1.24.2, 10.1.24.4,
10.2.22.2, 10.2.22.6
                   (0/6 fails/tries, stratum 2)
                   (0/0 fails/tries, stratum 2)
                   (0/0 fails/tries, stratum 2)
                   (0/0 fails/tries, stratum 2)
...

```

Any errors resulting from polling or synchronization are written to syslog messages.

## Example: Configuring Encrypted Management Sessions

While the serial management sessions are secure due to their nature, they are not always convenient. You can set a passphrase and encryption method for remote configuration sessions to secure them.

- Initiate a serial management session, and enter Privileged and Configuration modes.

```
myDevice> enable
myDevice# config
```



2. Set the remote management encryption method, selecting DES, and enter a passphrase (shared secret).

```
(config[myDevice])# remote-management encryption DES
(config[myDevice])# remote-management shared-secret
Enter shared secret:
Verify shared secret:
(config[myDevice])#
```

When you attempt to attach to the SSL appliance using the remote configuration manager, this prompt is displayed:

```
myDevice requires secure communication.
Enter passphrase for myDevice:
```

Enter the passphrase set previously.

You can change the TCP/UDP service port to be used when communicating with the device for management with the remote configuration manager. The TCP/UDP service port can be configured using any of the configuration connection options. You must save the configuration to flash and reboot for the port information to take effect.

```
(config[myDevice])# remote-management port 8089
(config[myDevice])# finished
myDevice# write flash
myDevice# reload
```

When the remote configuration manager is started, or the basic **discover** command is entered, the device is not found. You must enter the **discover** command using the TCP service port as an argument. The following command tells the configuration manager to use port 8089 to look for Cisco Secure Content Accelerator devices.

```
SCA> discover port 8089
```

The device is listed following a **show device list** command. Attach to the device configured in this example using the following command:

```
SCA> attach ip 10.1.2.3 port 8089
```

**Note**

---

If the device has been discovered by the Secure Content Accelerator, you can attach to it by name, e.g., **attach myDevice**.

---

If a passphrase has been configured for the device, you are prompted for it. Return the device management TCP service port by entering this command in Configuration mode:

```
(config[myDevice])# remote-management port default
```

## Example: Restricting Access using an Access List

Access lists permit or deny management access to the device or module. Up to 999 access lists can be configured. Access lists are created then assigned for use by the remote management, telnet, and Web management subsystems. An access list can be used by the SNMP subsystem as well. This example demonstrates how to create two access lists and assign each to a management subsystem.

1. Attach to the device or module (remote only) and enter Privileged and Configuration modes.

```
SCA> enable  
SCA> configure  
(config[myDevice])>
```

2. Create an access list allowing management access to all IP addresses.

```
(config[myDevice])> access-list 1 permit 0.0.0.0 255.255.255.255
```

3. Create an access list denying access from computers on a specific subnet.

```
(config[myDevice])> access-list 2 deny 10.1.3.0 0.0.0.255
```

4. Create an access list allowing access from a single computer.

```
(config[myDevice])> access-list 3 permit 10.1.4.5 0.0.0.0
```

5. Assign the second access list to the remote management subsystem.

```
(config[myDevice])> remote-management access-list 2
```

6. Assign the third access list to the telnet subsystem, allowing management access only from the specific IP address.

```
(config[myDevice])> telnet access-list 3
```

7. Exit to Privileged mode and save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
(config[myDevice])> finished
SCA> write flash
SCA>
```

**Note**

---

In FIPS Mode, access lists can be configured but assigned only to the SNMP subsystem.

---

## Configuring an Ethernet Interface

The Ethernet interfaces on the SSL appliance can be configured at either 10 Mbps or 100 Mbps and half or full duplex. Attach to the device (remote only) and enter Privileged and Configuration modes. In the following example, the “Network” interface of *myDevice* is forced to full duplex. Make sure to save this configuration to flash.

```
(config[myDevice])> interface network
(config-if[network])> duplex full
(config-if[network])> speed 100
(config-if[network])> finished
SCA>
```

## Step-Up Certificates and Server-Gated Cryptography

Cisco Secure Content Accelerator support both Netscape International Step-Up Certificates and Microsoft Server-Gated Cryptography. Ephemeral RSA must be enabled for the device to function properly with these certificates. Load the certificate normally.

**Note**

---

You must specify that your certificate work with both Microsoft and Netscape browsers when requesting it from the CA. Otherwise, the server cannot support both browsers.

---

# Configuring Certificate Groups

Certificate groups are collections of certificates used for certificate chains and client and server authentication. Certificate chains are used in certain circumstances such as when a known, trusted CA (such as Thawte or VeriSign) provides a certificate to attest that certificates created by an intermediary CA can be trusted. For example, a company can create its own certificates for internal use only; however, clients do not accept the certificates because they were not created by a known CA. When private certificates are chained with the trusted CA certificate, clients accept them during SSL negotiations.

## Example: Configuring a Certificate Group

The locally created certificate, the intermediary CA certificate signed by a trusted CA, and any other intermediary certificates are loaded into individual *certificate objects* that are combined into a *certificate group*. This example demonstrates how to:

- Load an intermediate CA certificate into a certificate object
- Create a certificate group
- Enable using the group as a certificate chain

The name of the SSL device is *myDevice*. The name of the secure logical server is *server1*. The name of the DER-encoded, intermediary CA certificate is *CACert*. The name of the PEM-encoded certificate generated by the intermediary CA is *localCertFile*. The name of the certificate group is *CACertGroup*.

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote only) and enter Privileged and Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice]>
```

3. Enter SSL Configuration mode and create an intermediary certificate named *CACert*, entering into Certificate Configuration mode. Load the DER-encoded file into the certificate object, and return to SSL Configuration mode.

```
(config[myDevice])> ssl
(config-ssl[myDevice])> cert CACert create
(config-ssl-cert[CACert])> der CACert
(config-ssl-cert[CACert])> end
(config-ssl[myDevice])>
```

4. Create a certificate named *localCert*, load the PEM-encoded certificate file, and return to SSL Configuration mode.

```
(config-ssl[myDevice])> cert localCert create
(config-ssl-cert[localCert])> pem localCertFile
(config-ssl-cert[localCert])> end
(config-ssl[myDevice])>
```

5. Enter Certificate Group Configuration mode, create the certificate group *CACertGroup*, load the certificate object *CACert*, and return to SSL Configuration mode.

```
(config-ssl[myDevice])> certgroup CACertGroup create
(config-ssl-certgroup[CACertGroup])> cert CACert
(config-ssl-certgroup[CACertGroup])> end
(config-ssl[myDevice])>
```

6. Enter Server Configuration mode, create the logical secure server *server1*, assign an IP address, SSL and clear text ports, a security policy *myPol*, the certificate group *CACertGroup*, certificate *localCert*, key *localKey* (compatible with the local certificate), and exit to Privileged mode.

```
(config-ssl[myDevice])> server server1 create
(config-ssl-server[server1])> ip address 10.1.2.4
(config-ssl-server[server1])> localport 443
(config-ssl-server[server1])> remoteport 81
(config-ssl-server[server1])> secpolicy myPol
(config-ssl-server[server1])> certgroup chain CACertGroup
(config-ssl-server[server1])> cert localCert
(config-ssl-server[server1])> key localKey
(config-ssl-server[server1])> finished
SCA>
```

7. Save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
SCA> write flash
SCA>
```

## Example: Importing Certificate Groups

PKCS#7 certificate groups can be imported directly into the device. This example demonstrates how to import a PEM-encoded PKCS#7 file into the Cisco Secure Content Accelerator.

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote only) and enter Privileged and Configuration modes.
3. Enter SSL Configuration mode.

```
(config[myDevice])> ssl
(config-ssl[myDevice])>
```

4. Specify the PKCS#7 file to import, indicating the appropriate encoding (in this example, PEM). In this example, the name of the certificate group to create is *myCertGroup*. The certificate prefix is *impt*. (The certificate prefix is optional.)

```
(config-ssl[myDevice])> import pkcs7 myCertGroup pem impt certfile.pem
```

5. The file is imported, and certificates and a certificate group are generated. The certificates are named incrementally from *impt\_1* to *impt\_N*, where *N* is the number of certificates in the PKCS#7 file. The certificate with the highest incremented number is the server certificate.



### Note

---

See the entry in Appendix C for additional command options.

---

# Using Client and Server Certificate Authentication

To further ensure transaction security, client or server certificate authentication can be configured on servers. Backend and reverse-proxy servers can be configured for server certificate authentication; basic secure servers can be configured for client certificate authentication. To use either of these certificate authentication methods, a certificate group must have been created.

## Example: Configuring Server Certificate Authentication

Server certification authentication can be configured on both backend and reverse-proxy servers. The configuration procedure for both server types is nearly identical. This example demonstrates how to configure an existing backend server for server certificate authorization using the certificate group *servTrustGroup*. The domain name (for backend server configuration only) is *www.mycorp.com*. Several options are available for authentication errors to ignore. In this example the backend server is set to not ignore errors, resulting in immediate disconnection.

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote devices only) and enter Privileged and Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])>
```

3. Enter SSL Configuration mode and Backend Server Configuration mode for the server *myBackServ*.

```
(config[myDevice])> ssl
(config-ssl[myDevice])> backend-server myBackServ
(config-ssl-backend[myBackServ])>
```

4. Enter the following commands to enable server certificate authentication, set the handling authentication of errors to the most stringent level, and assign the certificate group to use for comparison. (The final command must be entered on a single line.)

```
(config-ssl-backend[myBackServ])> serverauth enable  
(config-ssl-backend[myBackServ])> serverauth ignore none  
(config-ssl-backend[myBackServ])> certgroup serverauth  
servTrustGroup
```

5. Enter a domain name to use for certificate comparison. This is necessary only for backend servers when server certificate authentication is not set to ignore domain name errors. (The final command must be entered on a single line.)

```
(config-ssl-backend[myBackServ])> serverauth domain-name  
"www.mycorp.com"
```

6. Exit to Privileged mode, and save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
(config-ssl-backend[myBackServ])> finished  
SCA> write flash  
SCA>
```



## Example: Configuring Client Certificate Authentication

Client certification authentication can be configured on basic secure servers. This example demonstrates how to configure an existing server for client certificate authorization using the certificate group *clientTrustGroup*. Several options are available for authentication error handling. In this example, the server is set to handle all errors by disconnecting the SSL session and redirecting the client to a standard HTML error page.

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote devices only) and enter Privileged and Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])>
```

3. Enter SSL Configuration mode and Server Configuration mode for the server *myServ*.

```
(config[myDevice])> ssl
(config-ssl[myDevice])> server myServ
(config-ssl-server[myServ])>
```

4. Enter the following commands to enable client certificate authentication, set the handling of authentication of errors, and assign the certificate group to use for comparison.

```
(config-ssl-server[myServ])> clientauth enable
(config-ssl-server[myServ])> clientauth error all failhtml
(config-ssl-server[myServ])> certgroup serverauth clientTrustGroup
(config-ssl-server[myServ])> certgroup verifydepth 1
```

5. Exit to Privileged mode, and save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
(config-ssl-server[myServ])> finished
SCA> write flash
SCA>
```

# Generating Keys and Certificates

RSA private keys, certificates, and certificate signing requests can be generated directly on the device.

## Example: Generating an RSA Key

1. Enter Privileged, Configuration, SSL Configuration, and Key Configuration modes, creating a key named *myGenKey*.

```
SCA> enable
SCA> configure
(config[myDevice])> ssl
(config-ssl[myDevice])> key myGenKey create
(config-ssl-key[myGenKey])>
```

2. Enter the following command to generate a 1024-bit key using the seed string *lemon*. The key is displayed once using DES encryption. The resulting key is stored on the device as well as exported to a PEM-encoded file named *mykey.pem*. (This command must be entered on one line.)

```
(config-ssl-key[myGenKey])> genrsa bits 1024 encrypt des seed
lemon output mykey.pem
```

## Example: Generating a Certificate

1. Enter Privileged, Configuration, and SSL Configuration modes.

```
SCA> enable
SCA> configure
(config[myDevice])> ssl
(config-ssl[myDevice])>
```

2. Enter the following command to generate a certificate using the key created in the previous example. An MD5 digest is displayed and the certificate is saved in a file named *myGenCert*. (This command must be entered on one line.) A wizard starts, requesting certificate information.

```
(config-ssl[myDevice])> genscr key myGenKey digest md5 output
myGenCert
```

# Supporting SNMP

Cisco Secure Content Accelerator devices have basic support for SNMP functions. The device is shipped with SNMP disabled. This example demonstrates how to set basic SNMP data.

## Example: Configuring SNMP

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote only) and enter Privileged and Configuration modes.

```
SCA> enable
SCA> configure
```

3. Enter SNMP data and enable SNMP. *Access-list 1* has already been created. (See Appendix C for information for using the **access-list** command.) Return to Privileged mode.

```
(config[myDevice])> snmp enable
(config[myDevice])> snmp access-list 1
(config[myDevice])> snmp location "Main Office"
(config[myDevice])> snmp contact "Administrator"
(config[myDevice])> snmp default community ITS_Office
(config[myDevice])> snmp trap-host v1 10.1.2.4
(config[myDevice])> snmp trap-type generic
(config[myDevice])> end
SCA>
```

4. Save the configuration to flash memory. If not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
SCA> write flash
SCA>
```

# Supporting RIP

Cisco Secure Content Accelerator devices support Routing Information Protocol (RIP) versions 1 and 2. This example demonstrates how to enable RIP version 1 packet usage.

## Example: Configuring RIP

1. Initiate a management session as described previously.
2. Attach the configuration manager (remote only) and enter Privileged and Configuration modes.

```
SCA> enable
SCA> configure
```

3. Enable reception and processing of RIP version 1 packets. Then return to Privileged mode.

```
(config[myDevice])> rip v1
(config[myDevice])> end
SCA>
```

4. Save the configuration to flash memory. If not saved, the configuration is lost during a power cycle or if the **reload** command is used.

```
SCA> write flash
SCA>
```

## Supporting Other Secure Protocols

Along with SSL, Cisco Secure Content Accelerator devices can support other secure protocols using TLS v1.0, SSL v2.0, and SSL v3.0. IMAPS, POP3S, NNTPS, and LDAPS are some examples. The steps below show how to configure the SSL appliance for setting up a secure server to process only POP3S (S-POP) mail.

## Example: Configuring a Secure Mail Server

**Note**

---

The steps in this example are abbreviated to show only relevant changes from the standard SSL server setup.

---

1. Initiate a management session as described above. Attach the configuration manager to the device (remote only) and enter Privileged and Configuration modes. Enter a default router. Enter SSL Configuration mode.
2. Enter Server Configuration mode and create a server named *mySecureMail*. Assign an IP address and netmask. Assign port 995 for monitoring for POP3S (S-POP) connections and port 110 for sending clear text. Assign the appropriate key, certificate, and security policy. Return to Privileged mode.

```
(config-ssl[myDevice])> server mySecureMail create
(config-ssl-server[myServer])> sslport 995
(config-ssl-server[myServer])> remoteport 110
(config-ssl-server[myServer])> finished
SCA>
```

3. Save the configuration to flash memory. If not saved, the configuration is lost during a power cycle or when the **reload** command is used.

```
SCA> write flash
SCA>
```

## Supporting FIPS

Refer to Chapter 6, FIPS Operation, for instructions to use the Secure Content Accelerator in FIPS-compliant operation mode.





# Graphical User Interface Reference

---

This chapter describes how to use the Graphical User Interface (GUI) to configure the Cisco Secure Content Accelerator. The GUI provides a convenient, Web browser-based method of configuring the Secure Content Accelerator.



**Note**

---

The GUI cannot be used to configure the Secure Content Accelerator in FIPS Mode. See Chapter 6, Graphical User Interface Reference, for further information.

---

This chapter contains the following sections:

- Overview
- Browser and System Support
- Enabling Web Management
- Restricting Access to Web Management
- Starting the GUI
- Web Management User Interface
- General Configuration Examples
- SSL Configuration Examples
- Running the Secure Server Wizard

# Overview

While most configuration options are available with the GUI, you must be aware of the following constraints:

- The Secure Content Accelerator must have an IP address assigned before connecting with the GUI; use either serial configuration or the remote CLI to set the appliance IP information.
- The GUI cannot be used to set the SSL appliance to single-port operation.
- Web management must be enabled. See the command **web-mgmt** in Appendix C.

## Browser and System Support

The GUI has the following requirements:

- Color recommendations—The minimum display resolution required is SVGA (800x600 resolution). For best results, use XGA (1024x768 resolution).
- Browser Support—The GUI requires Microsoft® Internet Explorer version 5.x or later, or Netscape® Navigator 4.77 or 6.x or later.

## Enabling Web Management

Web management is disabled by default. To view the state of Web management, enter the **show device** CLI command. Web management status is shown in the returned listing as follows:

```
...  
Web Management:  disabled  
...
```

Enter Privileged and Configuration modes and enable Web management using these commands:

```
enable  
configure  
web-mgmt enable
```



The default TCP service port is 80. If you change it with the **web-mgmt port** command, you must use that port to connect with the device via the Web browser. Enter **show device** to check the state. The status should be listed similar to the following:

```
...  
Web Management:  enabled on port 80  
...
```

## Restricting Access to Web Management

We recommend that you restrict Web management access to the Secure Content Accelerator. Create one or more access lists using either the CLI (see “Example: Restricting Access using an Access List” in Chapter 4) or the GUI (as described later in this chapter.)

## Starting the GUI

Follow these steps to use the GUI to manage the Secure Content Accelerator.

1. Launch the Web browser.
2. When configuring a device in dual-port mode from a computer via the “Server” port, enter the SSL appliance IP address in the **Address** text box and press **Return** or **Enter**. If an enable password has been defined on the device, you are prompted for an user name and the enable password, as shown in Figure 5-1. Use “admin” for the user name. If no enable password has been configured, the GUI starts at the General content area.

Figure 5-1 Password Request Dialog Box

**Note**

Before configuring a device in two-port mode from the client side (via the “Network” port), you must first set up a secure server for this purpose. See “Configuring for Client-Side Access”.

## Configuring for Client-Side Access

Use the commands below as an example to set up a secure server named *web* on the Secure Content Accelerator, allowing GUI configuration from the client side (“Network” port).

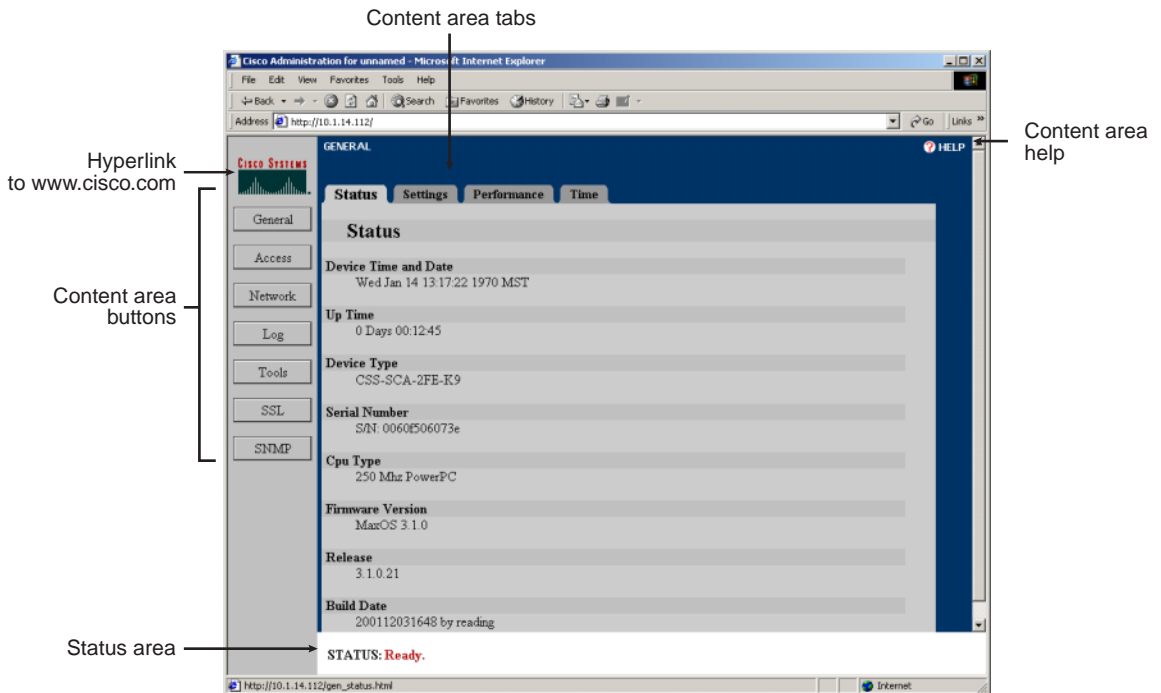
```
myDevice> attach
myDevice> enable
myDevice# configure
(config[myDevice])> ssl
(config-ssl[myDevice])> server web create
(config-ssl-server[web])> ip address 127.0.0.1
(config-ssl-server[web])> sslport 443
(config-ssl-server[web])> remoteport 80
(config-ssl-server[web])> no transparent
(config-ssl-server[web])> cert default-1024
(config-ssl-server[web])> key default-1024
(config-ssl-server[web])> secpolicy all
(config-ssl-server[web])> finished
myDevice#
```

Type **https://** and the IP address of the device in the **Address** text box of the browser, and press **Enter**. You receive a security alert dialog. Click **Yes** to proceed. If prompted, indicate that you wish to accept the certificate for this session only. You can proceed with configurations. You can also use the **Subsystem** tab in the **Access** content area to configure port access. Click the **HTTPS Service Enable** check box.

## Web Management User Interface

The GUI is divided into two main parts: the area panel on the left and content tabs on the right. Figure 5-2 shows an example of this interface. Take a few moments to familiarize yourself with the screen layout.

Figure 5-2 Basic User Interface Example



On the left is a panel with links to the seven main content areas.

- **General:** View general status, set device-specific information, view performance statistics, and set device time and date parameters
- **Access:** Set passwords, create and manage access lists, and specify subsystem access
- **Network:** Manage Ethernet interfaces, view network statistics, view ARP information, view and add to the routing table, view interface statistics and errors, view IP statistics, set DNS information
- **Log:** Set syslog message hosts and clear and view the device message log
- **Tools:** Reboot the device, manage running and startup configurations, update firmware, run diagnostic commands, and open a telnet connection with the device
- **SSL:** View SSL status and statistics and configure SSL (secure) servers, private keys, certificates, certificate chains, and security policies
- **SNMP:** View and configure SNMP traps and parameters

## General Configuration Examples

The following examples demonstrate how to use the GUI to configure general Secure Content Accelerator settings.



Note

---

To save time, make all the changes you wish, then click **Save to Flash** to write the configuration to the device flash memory.

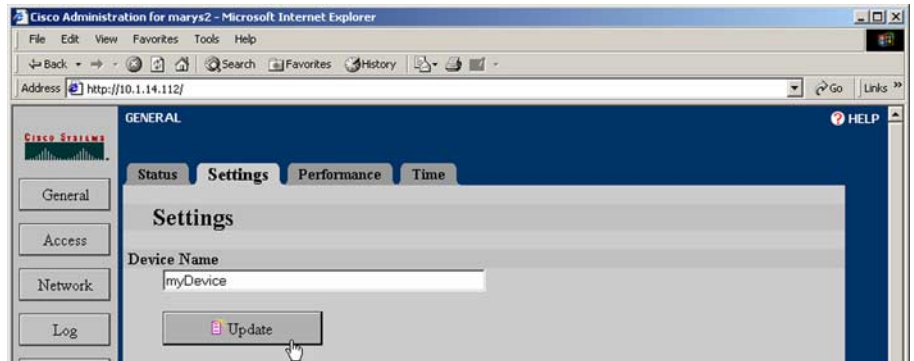
---

### Example: Setting the Device Name (Hostname)

Follow these steps to change the hostname of the device to *myDevice*.

1. Click **General** to activate the General content tabs.
2. Click the **Settings** tab. The **Settings** page opens, as shown in Figure 5-3
3. Type “myDevice” in the **Device Name** text box.

Figure 5-3 Changing Hostname Configuration Example

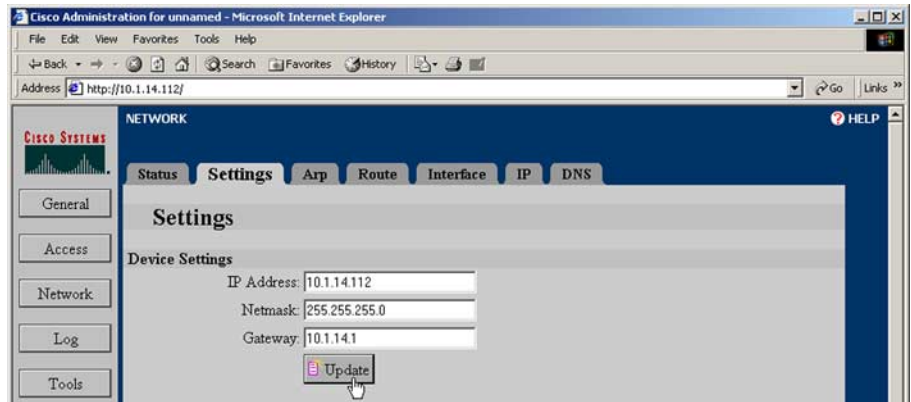


4. Click **Update**.

## Example: Resetting the IP Address

1. Click **Network** to activate the Network tabs.
2. Type the new IP address information including the appropriate netmask and default router in the **Internet Address**, **Netmask**, and **Gateway** text boxes, respectively, on the **Settings** tab. The **Settings** page opens, as shown in Figure 5-4.

Figure 5-4 Resetting IP Information Configuration Example



3. Click **Update**. The **Status** area tells you that the connection switches to the new address in 20 seconds.

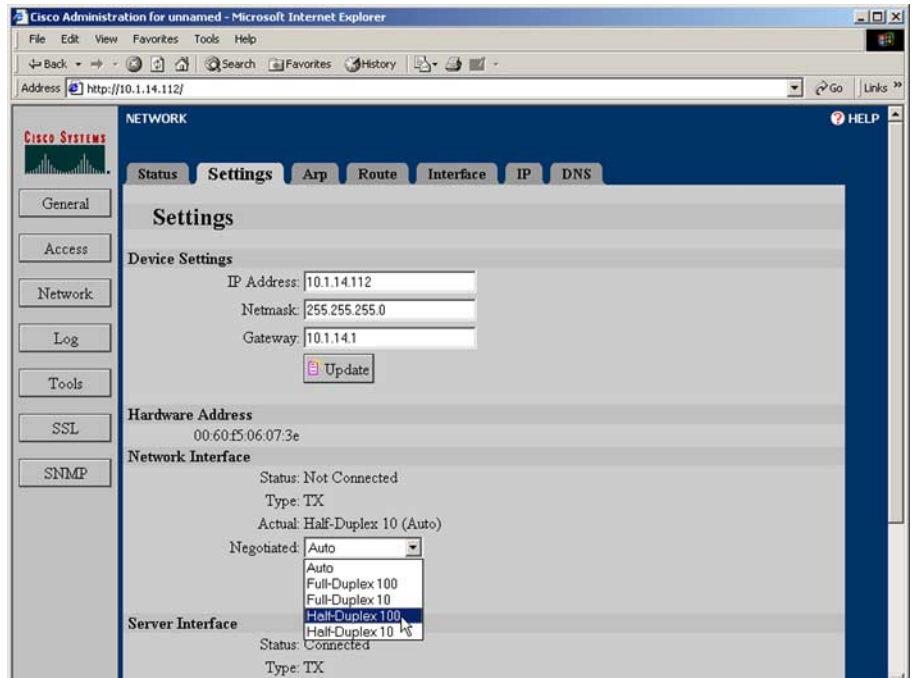
**Note**

In certain situations, such as when changing to a different subnet, redirection might not occur. If the connection is not redirected, manually connect to the device. If you still are unable to connect, use the serial configuration manager to check the device configuration and try again.

## Example: Configuring an Ethernet Interface

1. Click **Network** to activate the Network tabs.
2. Use the list box in the **Network Interface** or **Server Interface** panel of the **Settings** tab to change the Ethernet interface settings. The **Settings** page is shown in Figure 5-5.

Figure 5-5 Ethernet Interface Configuration Example

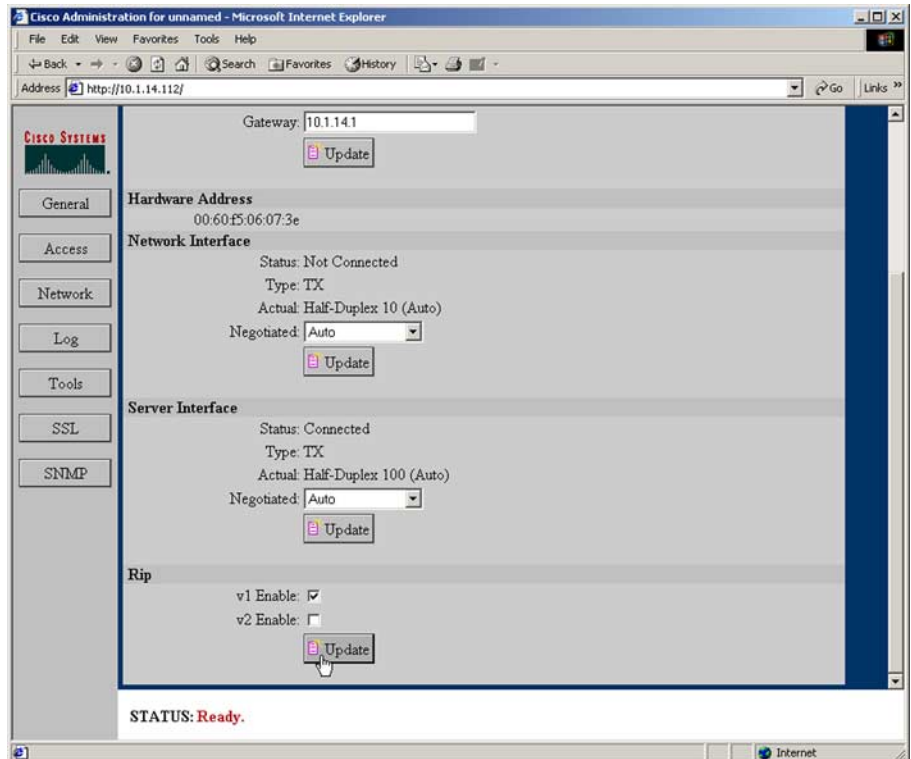


3. Click **Update**.

## Example: Enabling RIP

1. Click **Network** to activate the Network tabs.
2. Click the **Settings** tab. The **Settings** page opens, as shown in Figure 5-6.

Figure 5-6 RIP Configuration Example

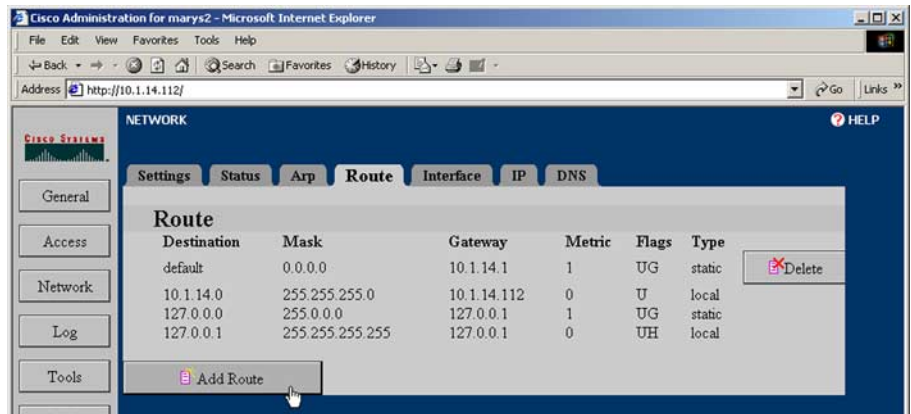


3. Scroll to the bottom of the page, if necessary, to see the **Rip** panel.
4. Select the **Enabled** check box.
5. Click **Update**.

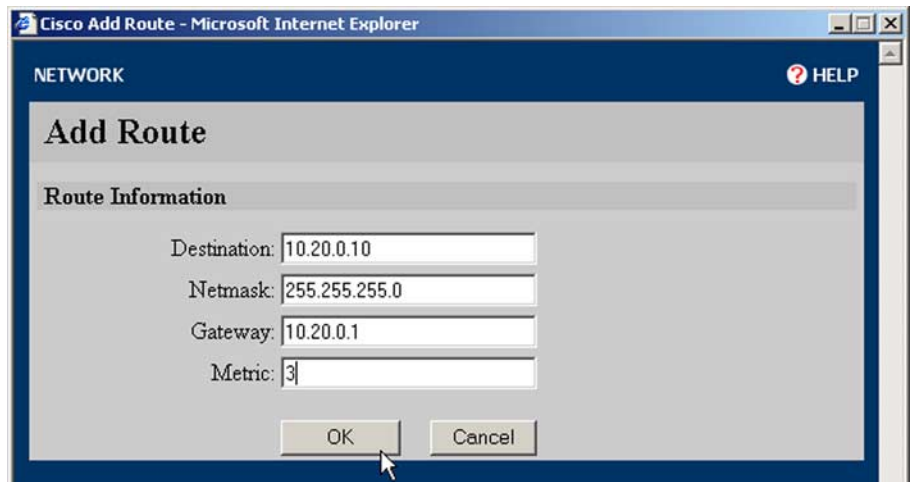
## Example: Adding a Route to the Routing Table

1. Click **Network** to activate the Network tabs.
2. Click the **Route** tab. The **Route** page opens, as shown in Figure 5-7.



**Figure 5-7 Routing Table Configuration Example**

3. Scroll to the bottom of the page, if necessary, to see the **Add Route** button.
4. Click **Add Route**. The **Add Route** window opens as shown in Figure 5-8.

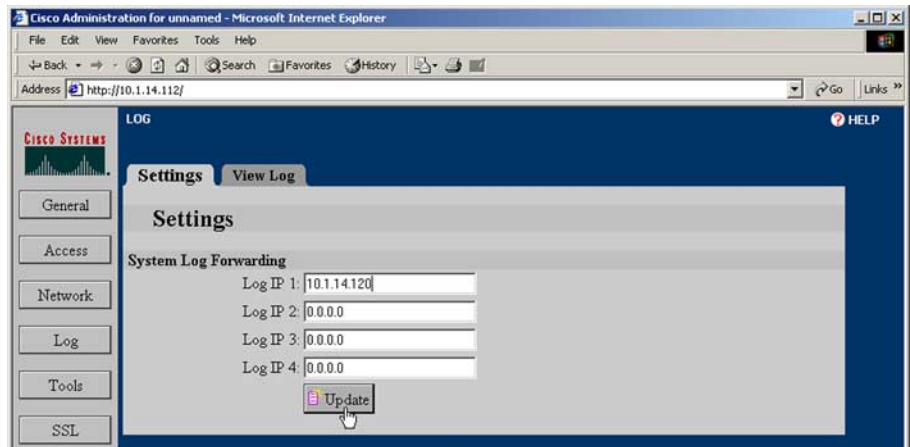
**Figure 5-8 Adding a Route Example**

5. Type the addressing and gateway information in the appropriate text boxes. Type the number of hops into the **Metric** text box.
6. Click **OK** to add the route or **Cancel** to close the window without adding the route information.

## Example: Working with Syslogs

1. Click **Log** to activate the Log tabs. The **Settings** page open automatically, as shown in Figure 5-9.

Figure 5-9 Syslog Configuration Example



2. Enter the IP addresses of the syslog hosts in the **System Log Forwarding** text boxes on the **Settings** tab.
3. Click **Update**.

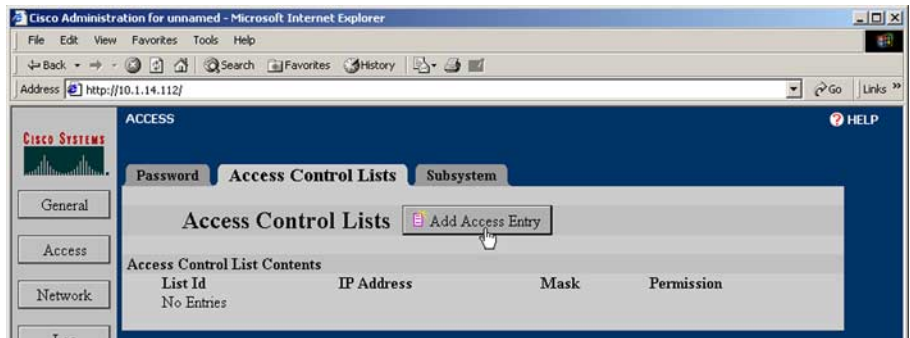
Use the **View Log** tab to display the syslog and clear the syslogs.

## Example: Restricting Access using an Access List

This example demonstrates how to set up an access list to permit management access to the Secure Content Accelerator.

1. Click **Access** to activate the Access tabs.
2. Click the **Access Control Lists** tab. The **Access Control Lists** page opens, as shown in Figure 5-10.

*Figure 5-10 Access List Configuration Example*

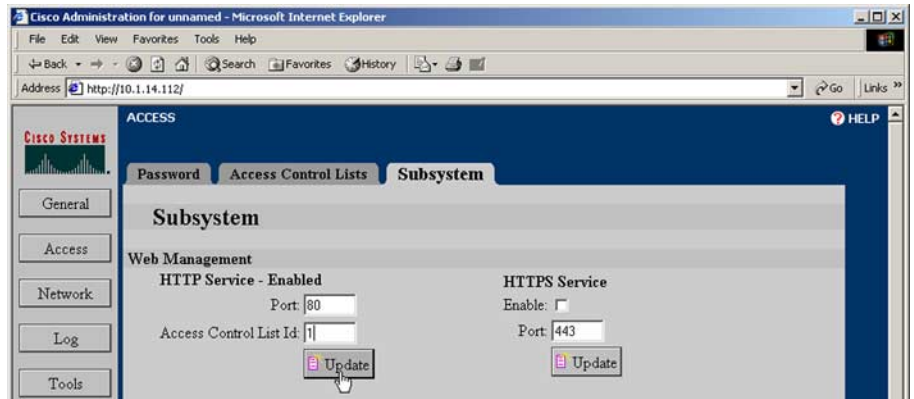


3. Click **Add Access Entry**. The **Add Access Control List** window opens, as shown in Figure 5-11.

*Figure 5-11 Add Access List Entry Example*

The screenshot shows a web browser window titled "Cisco Add Acl - Microsoft Internet Explorer". The page content is titled "ACCESS" and "Add Access Control List". Under the heading "Access Control List Information", there are four input fields: "Access Control List Id" with the value "1", "Permission" with a dropdown menu set to "Permit", "IP Address" with the value "10.1.14.110", and "Mask" with the value "0.0.0.255". At the bottom of the form are "OK" and "Cancel" buttons. A mouse cursor is pointing at the "OK" button.

4. Enter the appropriate information for the list entry. (See the **access-list** command in Appendix C for more information.)
5. Click **OK** to create the access list entry and close the window.
6. Click the **Subsystem** tab. The **Subsystem** page opens, as shown in Figure 5-12.

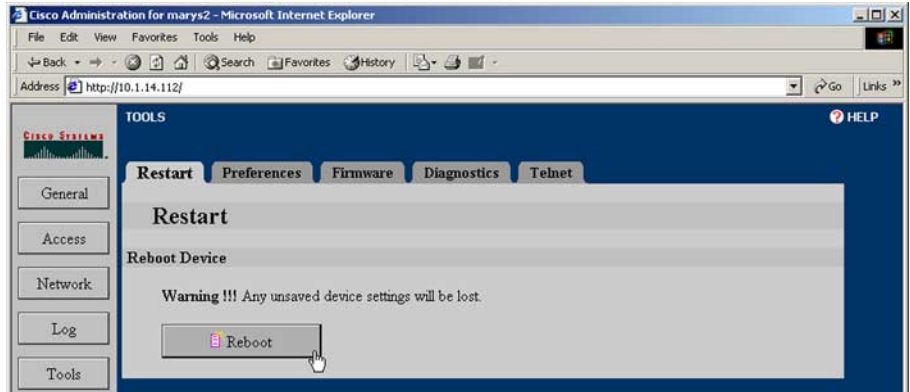
*Figure 5-12 Subsystem Access Configuration Example*

7. Type the number of the access list just created in the **Access Control List Id** text box of the **Web Management** panel. (You can also change the TCP port on this tab.)
8. Click **Update**.

## Example: Reloading (Rebooting) the Appliance

1. Click **Tools** to activate the Tools tabs. The **Restart** page opens automatically, as shown in Figure 5-13.

Figure 5-13 Device Reloading Example



2. If you have made changes to the device configuration but have not saved them to flash memory, click **Save to Flash** in the **Status** area, as shown in Figure 5-14.



### Caution

The appliance restarts using the configuration stored in flash memory. Any changes you have made but have not saved are lost.

Figure 5-14 Save Changes Button

**STATUS: Ready. The running configuration has been modified.** 

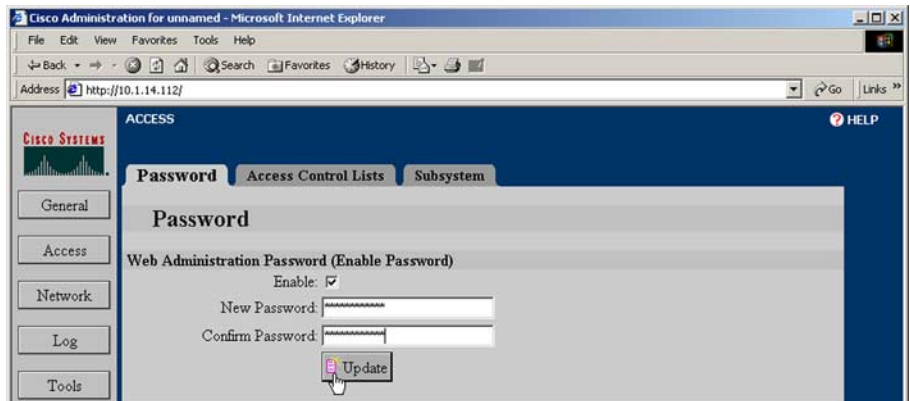
3. Click **Reboot** on the **Restart** page. The appliance reboots using the configuration stored in flash memory.

## Example: Setting an Enable Password

The Enable password is requested prior to connecting to the device.

1. Click **Access** to activate the Access tabs. The **Password** page opens automatically, as shown in Figure 5-15.

*Figure 5-15 Change Password Example*



2. If an Enable password has already been assigned, type it in the **Old Password** text box.
3. Type the password to use in the **New Password** text box, and retype it in the **Confirm New Password** text box.
4. Click **Update** to set the password.



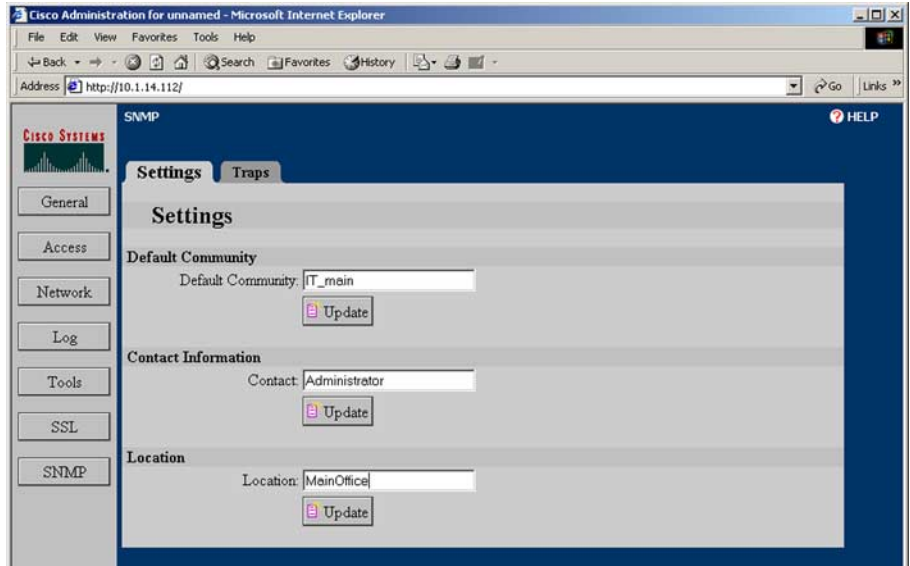
### Note

To remove an existing Enable password entirely, clear the **Enable** checkbox, type the existing password in the **Old Password** text box. Click **Update**.

## Example: Configuring SNMP

1. Click **SNMP** to activate the SNMP tabs. The **Settings** page opens automatically, as shown in Figure 5-16.

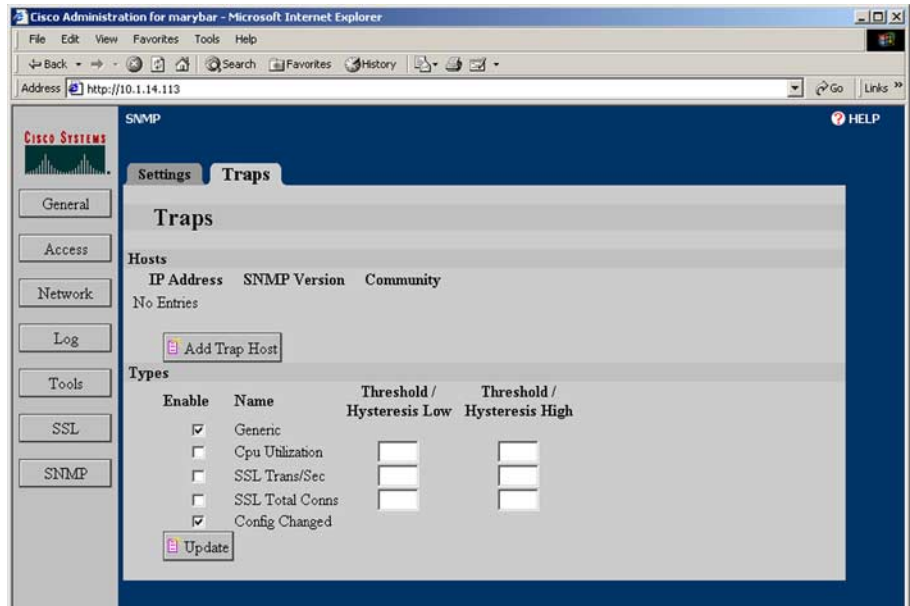
Figure 5-16 SNMP Configuration Example



2. Type the default community, contact information, and location information in appropriate text boxes. Click **Update** after changing the value in each field and selecting the **Enabled** check box.
3. Click the **Traps** tab. The **Traps** page opens, as shown in Figure 5-17.



Figure 5-17 SNMP Trap Example



4. Click **Add Trap Host** to specify a host to which to send trapping messages. The **Add Trap Host** window opens, as shown in Figure 5-18.

Figure 5-18 Add SNMP Trap Host Example

The screenshot shows a web browser window titled "Cisco Add Trap Host - Microsoft Internet Explorer". The page content is a form titled "Add Trap Host" under the "SNMP" section. The form has a "Trap Host Information" section with the following fields:

- IP Address: 10.1.14.118
- SNMP Version: v1 (selected from a dropdown menu)
- Community: ITS\_Office

At the bottom of the form are two buttons: "OK" and "Cancel". A mouse cursor is pointing at the "OK" button.

5. Type the host IP address into the **IP Address** text box. If you wish the trap messages to be sent to a community other than the default community, enter the community name in the **Community** text box. Select the desired version of SNMP from the **SNMP Version** list box.
6. Click **OK** to add the trap host.
7. Set the desired traps by selecting the **Enable** option buttons and typing appropriate values in the **Threshold/Hysteresis Low** and **Hysteresis High** text boxes. If you wish to use only one trap point, enter a value only in the **Threshold/Hysteresis Low** text box.



**Note** Additional information is presented in the online Help for this tab. Click **Help** in the top right corner of the window.

8. Click **Update** to set the configuration.

# SSL Configuration Examples

The following examples demonstrate how to set up SSL configurations for the Secure Content Accelerator. If necessary, refer to Chapter 3 to see how the Secure Content Accelerator works with SSL protocol information.

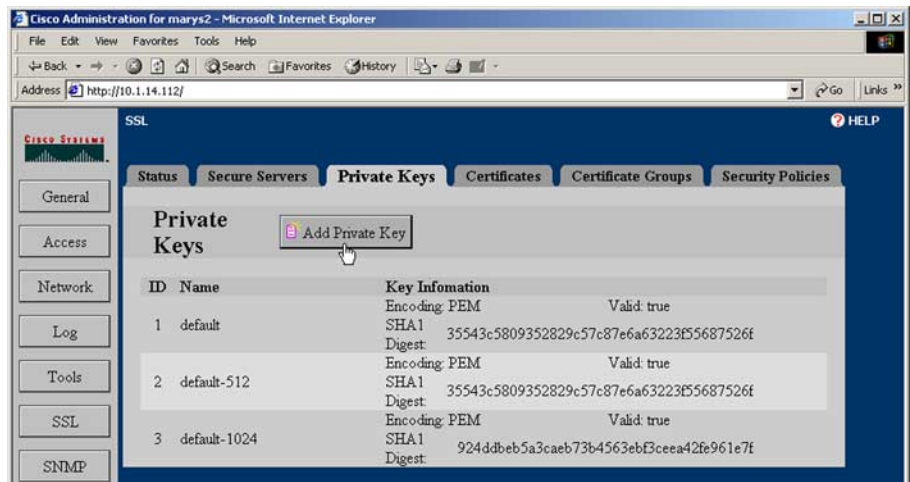
## Example: Setting up a Secure Server

In this example, the default SSL port (443) and remote port 81 are used. The user-specified key name is *myKey*, the certificate name is *myCert*, and the secure server name is *myServer*. The pre-loaded *strong* security policy is used.

The first step is to load a key to assign to the secure server. In this example, a key is imported into the GUI.

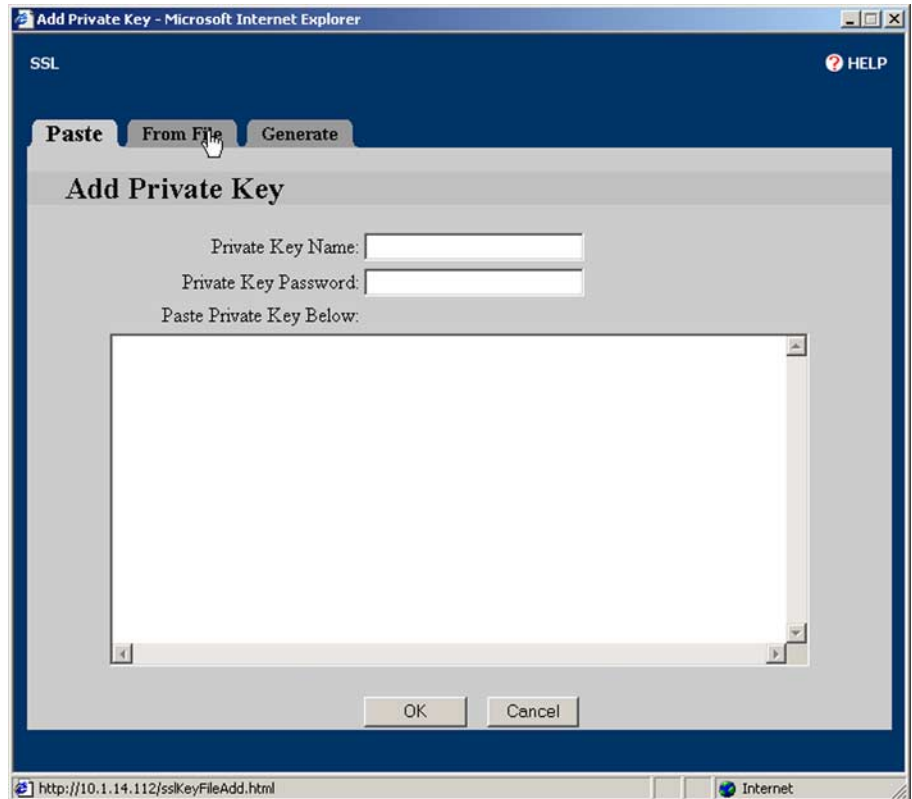
1. Click **SSL** to activate the SSL tabs.
2. Click the **Private Keys** tab. The **Private Keys** page opens, as shown in Figure 5-19.

Figure 5-19 Private Keys Tab



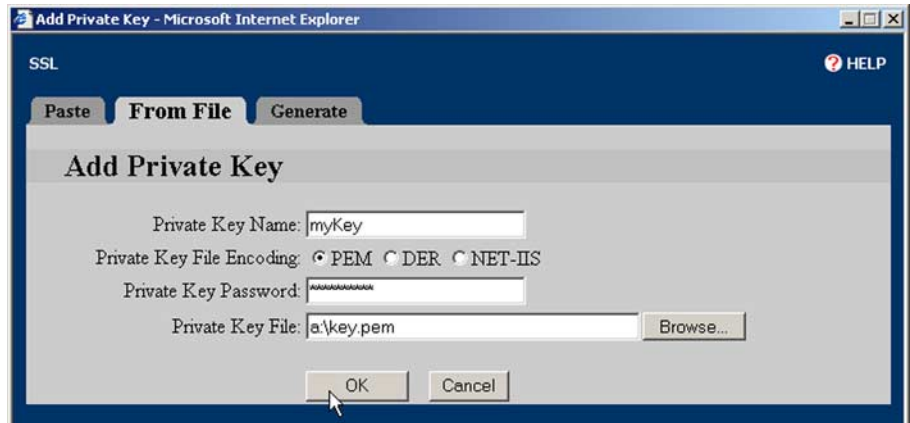
3. Click **Add Private Key**. The **Add Private Key** window opens, as shown in Figure 5-20.

*Figure 5-20 Add Private Key Example*



4. Click **From File**. The **From File** page opens, as shown in Figure 5-21. (In this example, the key is imported from a file. Alternatively, you can copy the key from the key file, and paste it into the **Paste Private Key Here** text box on the **Paste** tab. For an example of key generation, see “Example: Generating an RSA Private Key”.)

Figure 5-21 Importing a Private Key File Example



5. Type the key name, *myKey*, in the **Private Key Name** text box. Select the appropriate **Private Key File Encoding** option button. Type the password for the key in the **Private Key Password** text box. Enter the key file name and path or click the **Browse** button to find and select the file.
6. Click **OK** to load the key into the Secure Content Accelerator.  
Next, load a certificate to assign to the secure server. In this example, a certificate is imported into the GUI.
7. Click the **Certificates** tab. The **Certificates** page opens, as shown in Figure 5-22.

Figure 5-22 Certificates Tab

The screenshot shows the Cisco Administration GUI for an unnamed device, accessed via Microsoft Internet Explorer. The browser address bar shows `http://10.1.14.112/`. The page title is "Cisco Administration for unnamed - Microsoft Internet Explorer". The main navigation bar includes "Status", "Secure Servers", "Private Keys", "Certificates", "Certificate Groups", and "Security Policies". The "Certificates" tab is selected, and an "Add Certificate" button is visible.

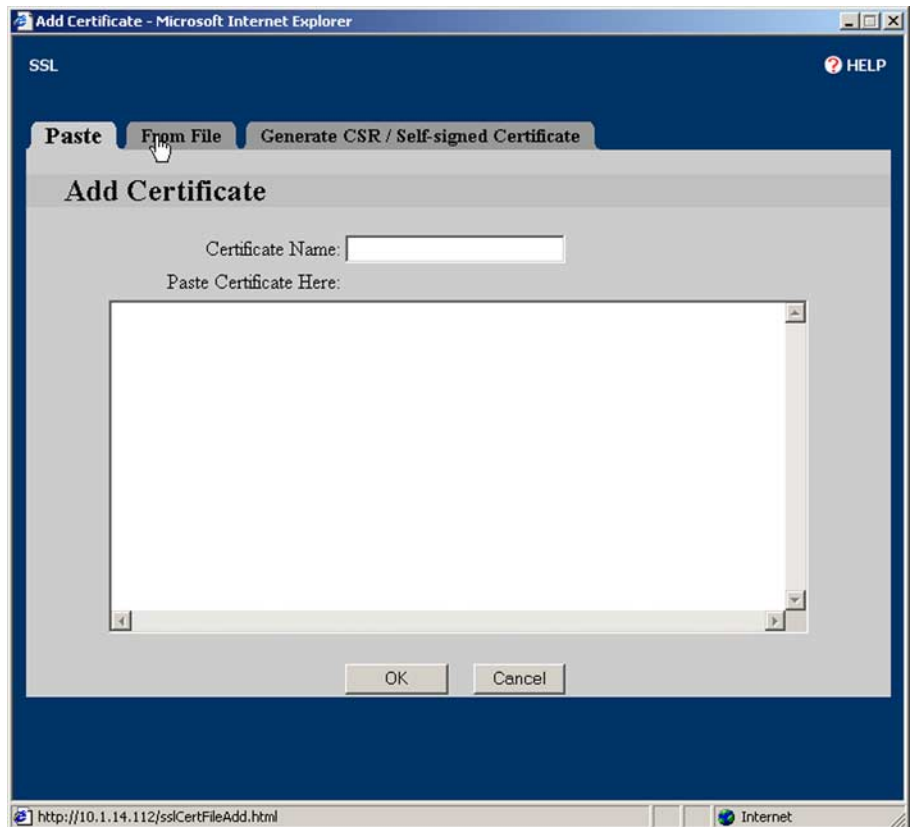
The left sidebar contains the following menu items: General, Access, Network, Log, Tools, SSL, and SNMP. The main content area displays a table of certificates:

ID	Name	Issuer Name	Subject Name	Valid
1	default	C=US ST=Dreamland L=Imaginary O=Illusionary Company Inc OU=Exaggerated Department CN=www.512key.delusionalfalsehood.org Email=noone@delusionalfalsehood.org	C=US ST=Dreamland L=Imaginary O=Illusionary Company Inc OU=Exaggerated Department CN=www.512key.delusionalfalsehood.org Email=noone@delusionalfalsehood.org	From: 9 May 2001 To: 3 Feb 2004
2	default-512	C=US ST=Dreamland L=Imaginary O=Illusionary Company Inc OU=Exaggerated Department CN=www.512key.delusionalfalsehood.org Email=noone@delusionalfalsehood.org	C=US ST=Dreamland L=Imaginary O=Illusionary Company Inc OU=Exaggerated Department CN=www.512key.delusionalfalsehood.org Email=noone@delusionalfalsehood.org	From: 9 May 2001 To: 3 Feb 2004
3	default-1024	C=US ST=Nowhere L=Void O=Non Existent Co. OU=Bogus Org. CN=www.1024key.controvertible.com Email=madeuppersons@controvertible.com	C=US ST=Nowhere L=Void O=Non Existent Co. OU=Bogus Org. CN=www.1024key.controvertible.com Email=madeuppersons@controvertible.com	From: 9 May 2001 To: 3 Feb 2004
4	DST__Baltimore_EZ...	C=US O=Digital Signature Trust Co. CN=Baltimore E? by DST	C=US O=Digital Signature Trust Co. CN=Baltimore E? by DST	From: 6 Jul 1999 To:

Below the table, the status is displayed as **STATUS: Ready.**

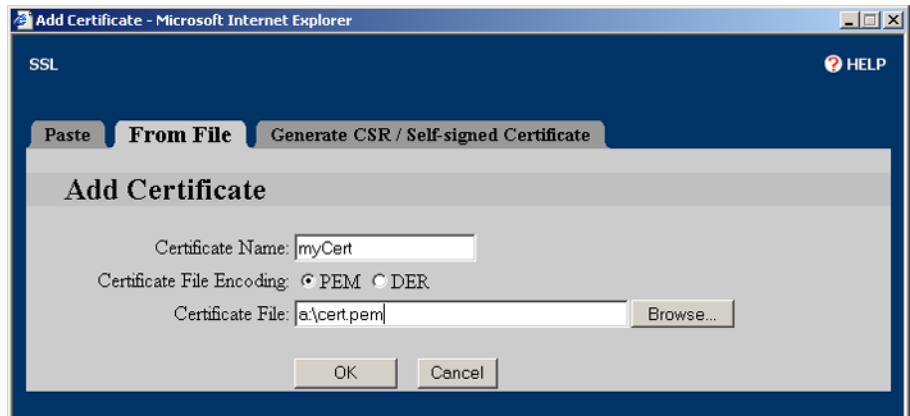
8. Click **Add Certificate**. The **Add Certificate** window opens, as shown in Figure 5-23.

*Figure 5-23 Add Certificate Example*



9. Click **From File**. The **From File** page opens, as shown in Figure 5-24. (In this example, the certificate is imported from a file. Alternatively, you can copy the certificate from the file, and paste it into the **Paste Certificate Here** text box on the **Paste** tab. For an example demonstrating certificate generation, see “Example: Generating a Self-Signed Certificate” below.)

*Figure 5-24 Importing a Certificate Example*



10. Type the certificate name, *myCert*, in the **Certificate Name** text box. Select the appropriate **Certificate File Encoding** option button. Enter the certificate file name and path or click the **Browse** button to find and select the file.
11. Click **OK** to load the certificate into the Secure Content Accelerator.

Several security policies are pre-loaded into the Secure Content Accelerator. You can use any of these or create your own policy when configuring a server. This examples demonstrates how to create a user-defined security policy.



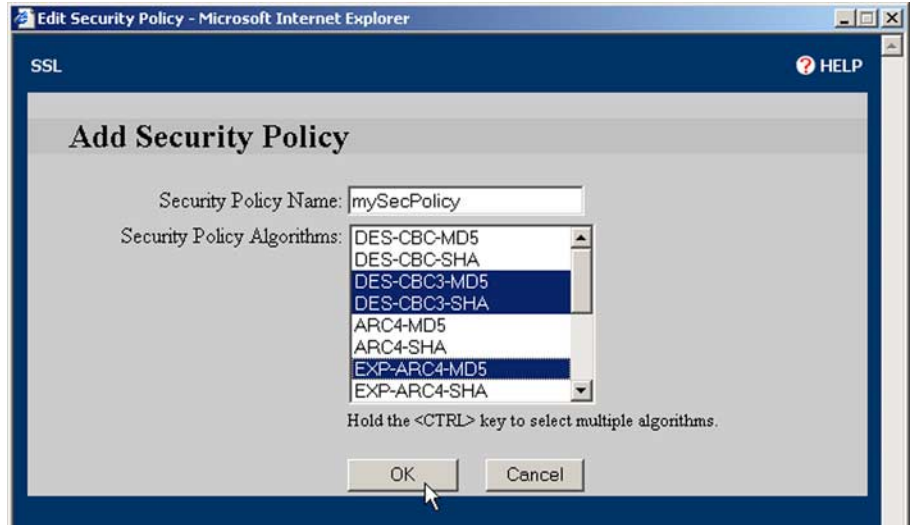
- Click the **Security Policies** tab. The **Security Policies** page opens, as shown in Figure 5-25.

*Figure 5-25 Security Policies Tab*



13. Click **Add Security Policy**. The **Add Security Policy** window opens, as shown in Figure 5-26.

*Figure 5-26 Add Security Policy Example*



14. Type the desired name in the **Security Policy Name** text box. Select the policies to include in the new security policy by clicking and **CTRL**+clicking the entries in the **Security Policy Algorithms** list box.
15. Click **OK** to create the policy.  
Now, set up the secure server.

- Click the **Secure Servers** tab. The **Secure Servers** page opens, as shown in Figure 5-27.

*Figure 5-27 Secure Servers Tab*



- Click **Add Secure Server**. The **Add Secure Server** window opens, as shown in Figure 5-28.

Figure 5-28 Add Secure Server Information Example

Secure Server - Microsoft Internet Explorer

SSL HELP

### Add Secure Server

**Secure Server Type**

- Normal Server** - Accepts SSL connections (listens) on the "SSL Port" and retransmits data to and from the clear text port.
- Backend Server** - Accepts clear-text connections on the "Clear-Text Port" and retransmits data to and from the SSL port.
- Reverse-Proxy Server** - Accepts clear-text HTTP connections on the device IP Address and retransmits to the HTTP defined destination URL from the device IP address and SSL Port.

**Secure Server Information (\* denotes a required field)**

Enable Secure Server:

Secure Server Name:  \*

IP Address:  \*

Clear-Text Port:  \*

SSL Port:  \*

Log Server:

Transparent Mode:

Redirect:

Ephemeral RSA:

**Server Certificate and Security Policy (\* denotes a required field)**

Certificate:  \*

18. Choose the type of secure server to create by clicking the appropriate option button. (This example configures a Normal Server.) Type the server name, *myServer*, in the **Secure Server Name** text box. Type the IP address of the server to which to send decrypted SSL traffic in the **IP Address** text box. Change the **Clear-Text Port** to "81".
19. Scroll to the **Server Certificate and Security Policy** panel. Select *myCert* from the **Certificate** list box. Select *myKey* from the **Private Key** list box. Select *strong* from the **Security Policy** list box. These options are shown in Figure 5-29.

**Figure 5-29 Server Certificate and Security Policy Example**

Server Certificate and Security Policy (\* denotes a required field)

Certificate: myCert \*

Private Key: myKey \*

Security Policy: strong \*

Certificate Group - Server Chain: -NotUsed-

20. Select the desired options in the **Client Certificate Authentication** panel, shown in Figure 5-30.

**Figure 5-30 Add Secure Server Information Example**

Client Certificate Authentication (optional)

Client Authentication:  Off  On

Certificate Group - Client Trust: defaultCA

Verification Depth: 2

**Error Handling**

Certificate Not Provided: Fail [All](#)

Certificate Not Yet Valid: Fail [All](#)

Certificate Has Expired: Fail [All](#)

Certificate Revoked: Fail [All](#)

Certificate Has Invalid CA: Fail [All](#)

Certificate Has Signature Failure: Fail [All](#)

Other Errors: Fail [All](#)

21. Set up Secure URL Rewrite for the server, if desired. Enter the domain name (including wildcard, if appropriate) in the **URL Clear-Text Port** text box. Edit the port definitions, if necessary. Click **Add**, as shown in Figure 5-31, to define the URL rewrite rule.

Figure 5-31 Add URL Rewrite Rule Example

Use the **Rewrite “HTTP 3xx” Header Only** check box to indicate only 30x-series redirects referencing http:// rather than all instances of http:// (such as those appearing intentionally in the application data) be rewritten.



**Note** For more information, see the “Example: Configuring Secure URL Rewrite” section on page 4-17

22. Click **OK** to create the secure server on the Secure Content Accelerator.

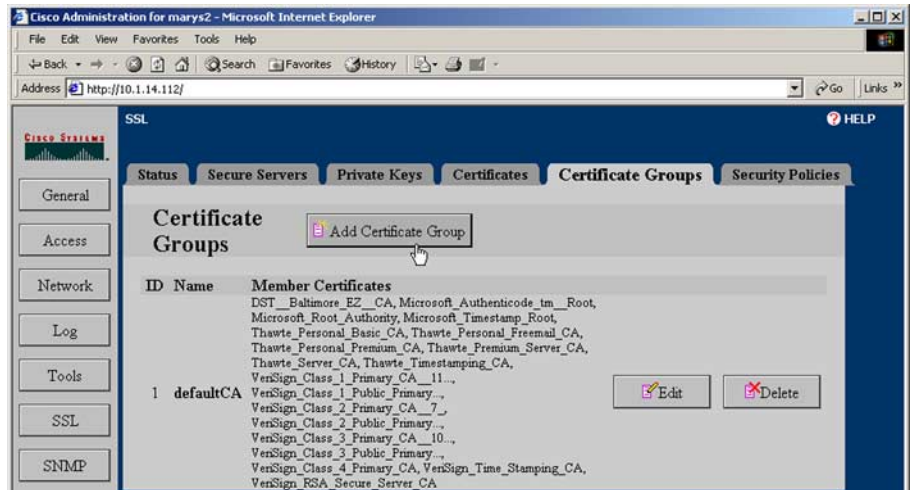
The same procedures are used to create and edit backend servers and reverse-proxy servers. Options presented in the window change, depending upon the type of server being configured.

## Example: Creating and Using Certificate Groups

This example demonstrates how to select certificates already loaded in the Secure Content Accelerator to create a certificate group. Alternatively, a PKCS#7 certificate group can be imported directly. See “ Example: Importing a PKCS#7 Certificate Group”, below, for a demonstration.

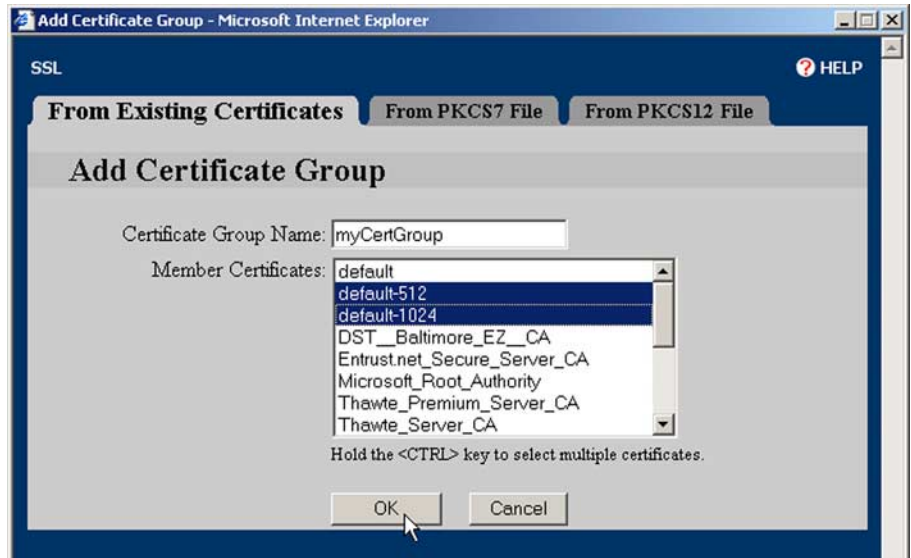
1. Click **SSL** to activate the SSL tabs.
2. Click the **Certificate Groups** tab. The Certificate Groups page is shown in Figure 5-32.

Figure 5-32 Certificate Groups Tab



3. Click **Add Certificate Group**. The **Add Certificate Group** window opens, as shown in Figure 5-33.

*Figure 5-33 Add Certificate Group Example*



4. Type the name for the group in the **Certificate Group Name** text box.
5. Click and **CTRL**+click the certificates listed in the **Member Certificates** list box to add to the certificate group. You can also click and **SHIFT**+click either end of a contiguous group of certificates to select all certificates in it.
6. Click **OK** to add the certificate group to the device.

Follow the steps below to assign the certificate group to a secure server.

1. Click **SSL** to activate the SSL tabs.
2. Click the **Secure Servers** tab.
3. Either click **Edit** next to an existing secure server, or click **Add Secure Server** to create a new server. The appropriate secure server window opens.
4. Locate the **Server Certificate and Security Policy** panel.



5. Select “myCertGroup” from the **Certificate Group - Server Chain** list box. These options are shown in Figure 5-34.

**Figure 5-34 Assign Certificate Group Example**

6. Click **OK** to add the new configuration.



**Note**

---

If you are creating a new secure server, you must complete configuring the server as presented previously in this chapter.

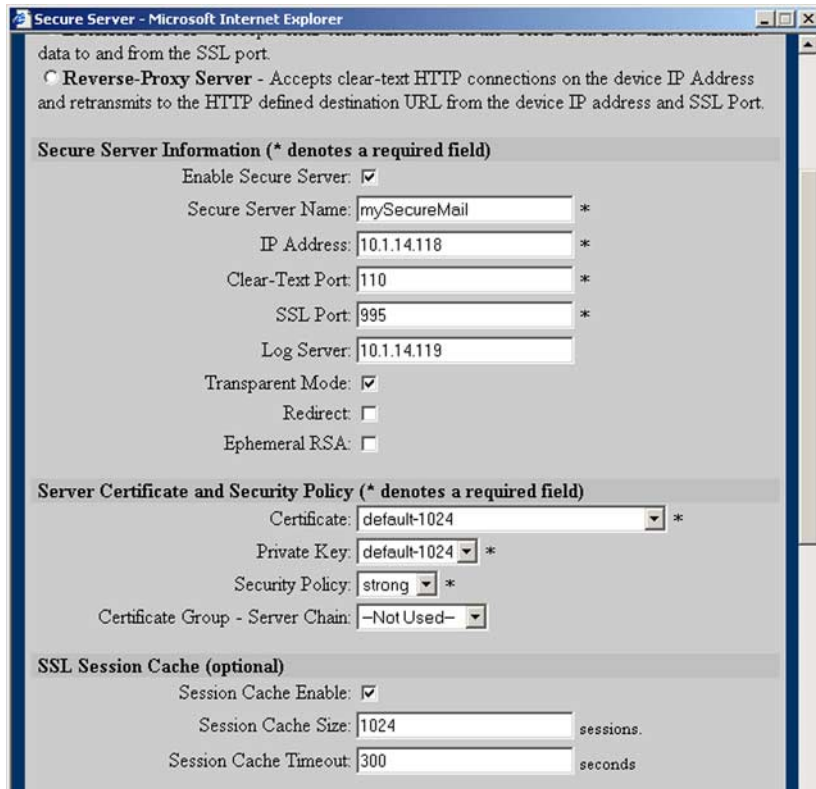
---

## Example: Supporting Other Secure Protocols

The Secure Content Accelerator can be used for protocols other than pure SSL applications. In this example, a secure server is set up to process only POP3S (S-POP) mail.

1. Click the **Secure Servers** tab.
2. Click **Add Secure Server**. The **Add Secure Server** window opens.
3. Type the server name, *mySecureMail*, in the **Secure Server Name** text box. Type the IP address of the server to which to send decrypted SSL traffic. Type “110” in the **Remote Port** text box. Type “995” in the **SSL Port** text box. Select **strong** from the **Security Policy** list box. Select **default-1024** from the **Certificate** list box. Select **default-1024** from the **Private Key** list box. These options are shown in Figure 5-35.

Figure 5-35 Configuring for Other Protocols Example



data to and from the SSL port.

**Reverse-Proxy Server** - Accepts clear-text HTTP connections on the device IP Address and retransmits to the HTTP defined destination URL from the device IP address and SSL Port.

**Secure Server Information (\* denotes a required field)**

Enable Secure Server:

Secure Server Name:  \*

IP Address:  \*

Clear-Text Port:  \*

SSL Port:  \*

Log Server:

Transparent Mode:

Redirect:

Ephemeral RSA:

**Server Certificate and Security Policy (\* denotes a required field)**

Certificate:  \*

Private Key:  \*

Security Policy:  \*

Certificate Group - Server Chain:

**SSL Session Cache (optional)**

Session Cache Enable:

Session Cache Size:  sessions.

Session Cache Timeout:  seconds

4. Click **OK** to create the secure server in the Secure Content Accelerator.

## Example: Generating an RSA Private Key

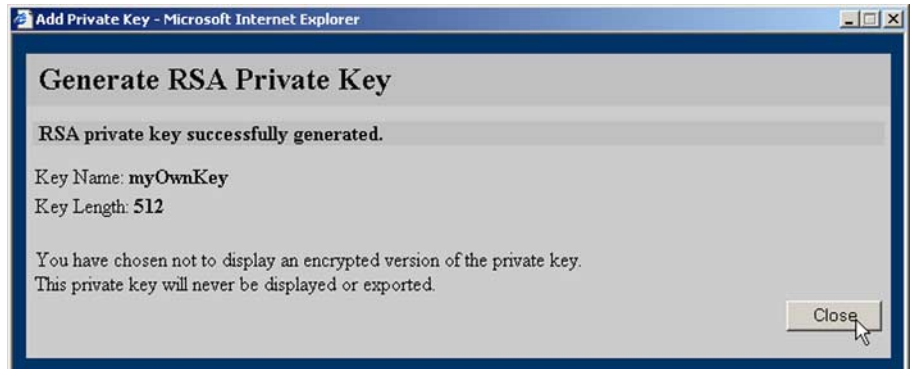
This example demonstrates how to generate an RSA private key named *myOwnKey*.

1. Click **SSL** to activate the SSL tabs.
2. Click **Add Private Key**. The **Add Private Key** window opens.
3. Click the **Generate** tab. The **Generate an RSA Private Key** window opens, as shown in Figure 5-36.

Figure 5-36 Generating a Private Key

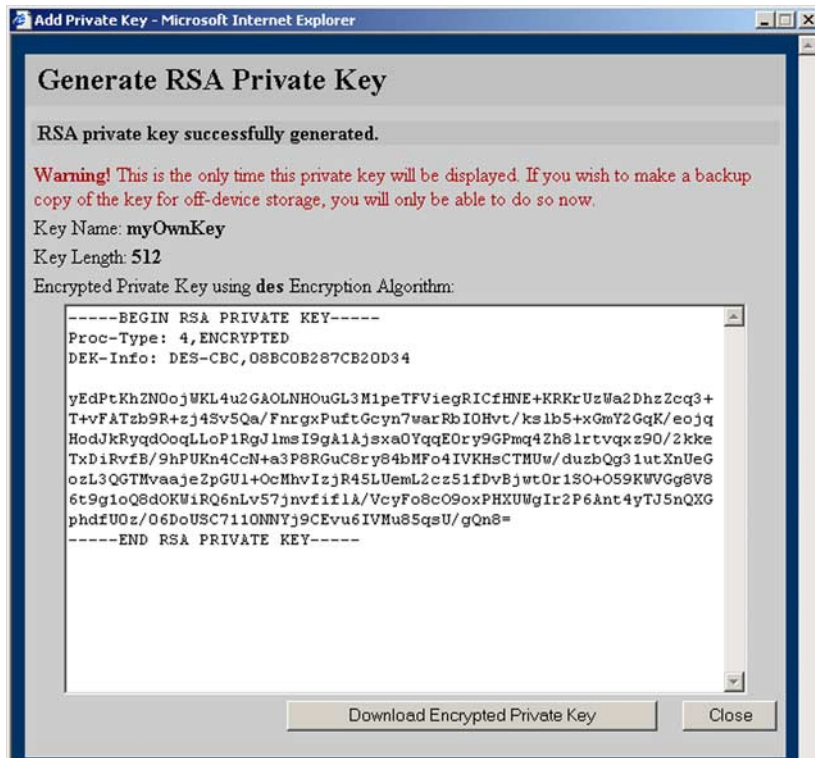


4. Type “myOwnKey” in the **Private Key Name** text box.
5. Select **512 bits** from the **Private Key Length** list box. This value is proportionate to the strength of the key.
6. If you want to specify any additional seed data for the random number generator, type it into the **Extra Random Number Generator Seed Data** text box.
7. Choose an option in the **Display Encrypted Key for Backup** list box.
  - **Do Not Display Key:** The private key is never displayed. You cannot save the key to a file for backup purposes.
  - **Display key using Des Encryption:** The private key is displayed using DES encryption and can be saved to a file.
  - **Display key using Des3 Encryption:** The private key is displayed using 3DES encryption and can be saved to a file.
8. Click **OK**. Depending upon the selection made from the **Display Encrypted Key for Backup** list box, one of two windows opens:
  - If **Do Not Display Key** was selected, the key is generated and a window opens, reminding you that the key cannot be displayed or exported. This is shown in Figure 5-37. Click **Close**.

*Figure 5-37 Key Not Displayed Example*

- If either **Display key using Des Encryption** or **Display key using Des3 Encryption** were selected, the key is generated and a window opens, displaying the encrypted key. This is shown in Figure 5-38. Click **Download Encrypted Private Key** to make a backup copy of the key, if desired. Click **Close**.

Figure 5-38 Key Displayed Example



## Example: Generating a Self-Signed Certificate

This example demonstrates how to generate a certificate signing request (CSR) and a self-signed certificate.

1. Click **SSL** to activate the SSL tabs.
2. Click the **Certificates** tab.
3. Click **Add Certificate**. The **Add Certificate** window opens.
4. Click the **Generate CSR/Self-signed Certificate** tab. The **Generate CSR/Self-signed Certificate** page opens, as shown in Figure 5-39.

Figure 5-39 Generate CSR Example

The screenshot shows the 'Add Certificate' dialog box in Microsoft Internet Explorer. The title bar reads 'Add Certificate - Microsoft Internet Explorer'. The main window has a dark blue header with 'SSL' and a 'HELP' icon. Below the header is a grey bar with the title 'Add Certificate'. The main content area has three tabs: 'Paste', 'From File', and 'Generate CSR / Self-signed Certificate'. The 'Generate CSR / Self-signed Certificate' tab is active, showing a form titled 'Generate a Certificate Signing Request (CSR) / Self-signed Certificate'. The form contains the following fields and values:

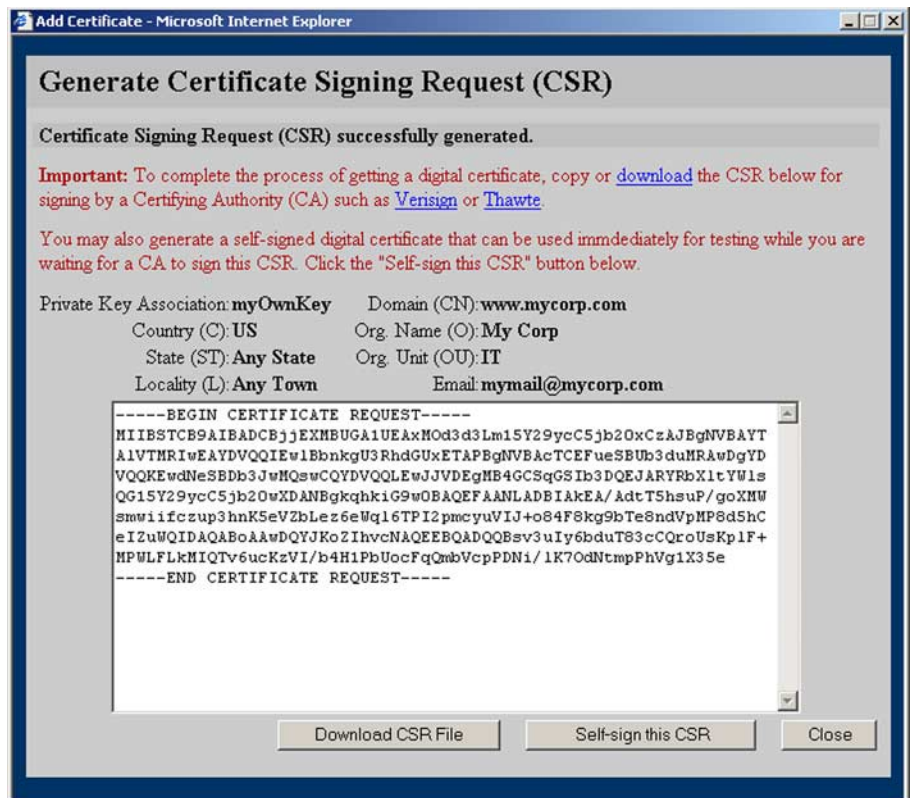
- Private Key Association: myOwnKey (dropdown)
- Domain Name (CN): www.mycorp.com (text box, Example: www.example.com)
- Country (C): US (text box, Example: US)
- State (ST): Any State (text box, Example: California)
- Locality (L): Any Town (text box, Example: San Jose)
- Organization Name (O): My Corp (text box, Example: Example Corporation)
- Organizational Unit (OU): IT (text box, Example: IT Department)
- Email Address (Email): mymail@mycorp.com (text box, Example: admin@example.com)
- CSR Message Digest: MD5 (dropdown)
- CSR Header: BEGIN CERTIFICATE REQUEST (dropdown)

At the bottom of the form, there is a note: 'Note: Some older Certifying Authorities (CAs) require "NEW" in the CSR header.' Below the note are 'OK' and 'Cancel' buttons.

5. Select the key to associate with the certificate from the **Private Key Association** list box.

6. Enter the desired domain name, country, state, locality, organization name, organization unit, and e-mail address in the appropriate text boxes.
7. Select the appropriate message digest format for the signing request from the **CSR Message Digest** list box.
8. Select the appropriate header from the **CSR Header** list box.
9. Click **OK**. The certificate is created and the **Generate Certificate Signing Request (CSR)** opens, as shown in Figure 5-40.

Figure 5-40 Generate Self-Signed Certificate



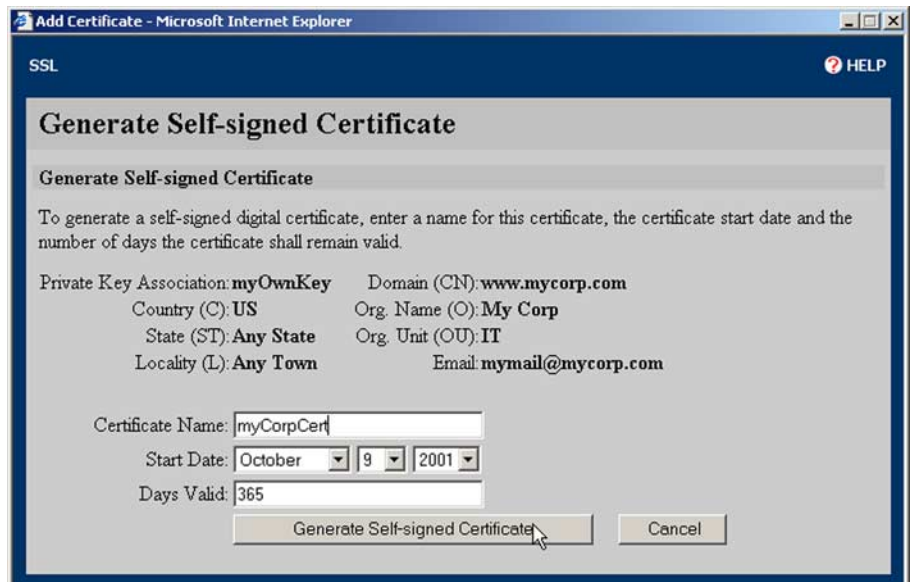
- Click **Download CSR File** to save the file to the local file system for transfer to the Certificate Authority.



**Note** If you know the preferred file name convention of the CA, name the file appropriately now. Otherwise, accept the default naming convention and rename the file later if necessary.

- Click **Self-sign this CSR** to generate a self-signed digital certificate to be used for testing while you wait for the certificate to be signed. The **Generate Self-signed Certificate** window opens, as shown in Figure 5-41.

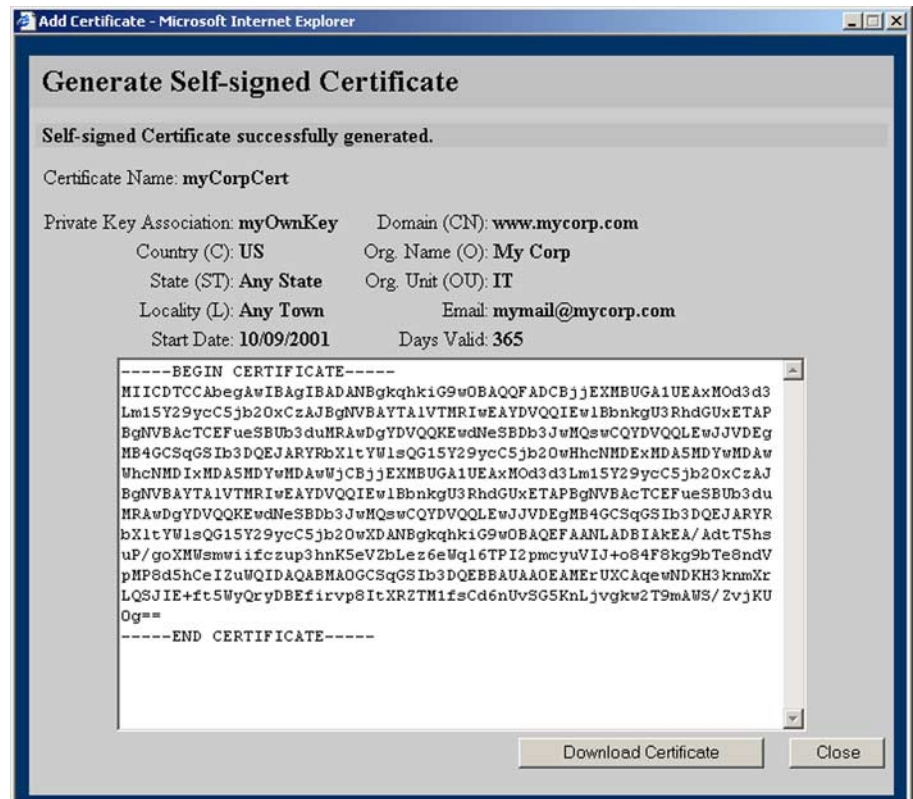
*Figure 5-41 Self-Signed Certificate Example*





12. Type the name for the certificate in the **Certificate Name** text box. Select the appropriate date to begin validity of the certificate from the **Start Date** list boxes. Change the number of days the certificate is valid in the **Days Valid** text box, if desired. Click **Generate Self-signed Certificate**. The certificate is generated, and a window opens, allowing the certificate to be downloaded. The **Generate Self-signed Certificate** window is shown in Figure 5-42. Click **Close**.

Figure 5-42 Successfully Generated Self-Signed Certificate

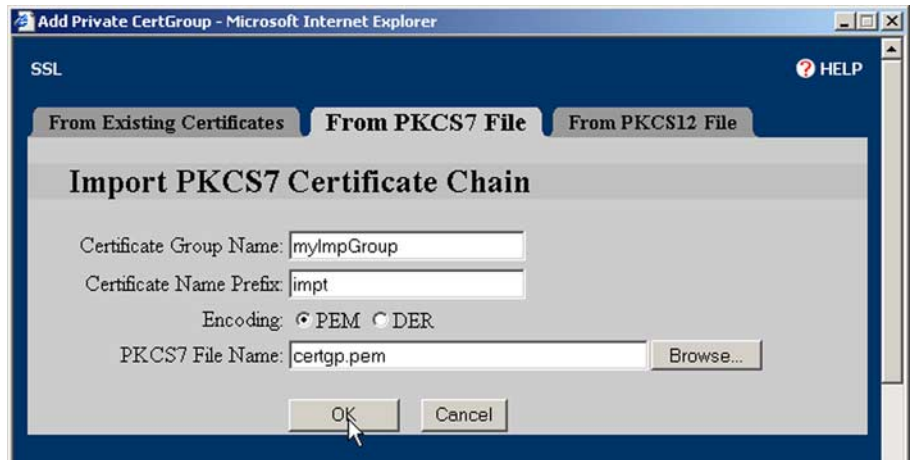


## Example: Importing a PKCS#7 Certificate Group

This example demonstrates how to import a PKCS#7 certificate group into the Secure Content Accelerator.

1. Click **SSL** to activate the SSL tabs.
2. Click the **Certificate Groups** tab.
3. Click **Add Certificate Group**. The **Add Certificate Group** window opens.
4. Click the **From PKCS7 File** tab. The **Import PKCS7 File** page opens, as shown in Figure 5-43.

Figure 5-43 Import PKCS#7 Certificate Group Example



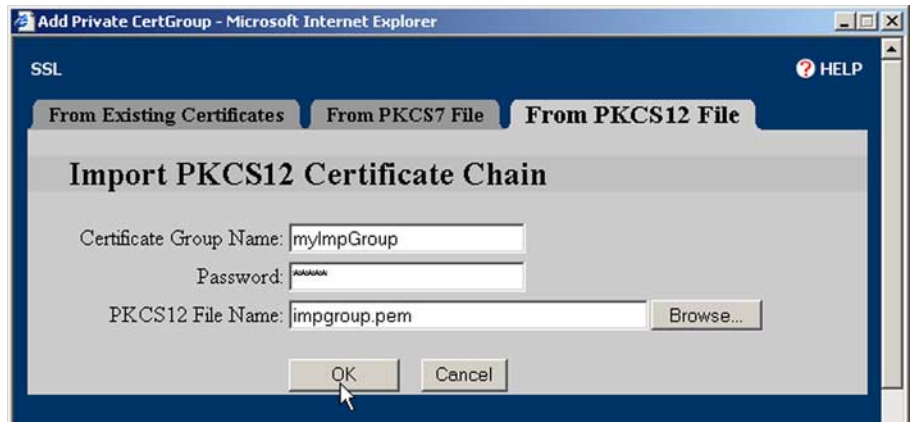
5. Type the name of the group in the **Certificate Group Name** text box.
6. Type the base name of the certificate in the **Certificate Name Prefix** text box.
7. Select the encoding option for the file to import by clicking the appropriate **Encoding** option button.
8. Either type the name and path of the PKCS#7 file to import, or click **Browse** and navigate to and select the file.
9. Click **OK**.

## Example: Importing a PKCS#12 Certificate Group

This example demonstrates how to import a PKCS#12 certificate group into the Secure Content Accelerator.

1. Click **SSL** to activate the SSL tabs.
2. Click the **Certificate Groups** tab.
3. Click **Add Certificate Group**. The **Add Certificate Group** window opens.
4. Click the **From PKCS12 File** tab. The **Import PKCS12 Certificate Chain** window opens, as shown in Figure 5-44.

Figure 5-44 Import PKCS#12 Certificate Group Example



5. Type the name of the group in the **Certificate Group Name** text box.
6. Type the key password in the **Password** text box.
7. Either type the name and path of the PKCS#12 file to import, or click **Browse** and navigate to and select the file.
8. Click **OK**.

# Running the Secure Server Wizard

The Secure Server wizard can be executed from the GUI. The wizard steps you through the basic SSL secure server configuration, but it does not provide all the features of either the GUI or CLI alone.

1. Click **SSL** to activate the SSL tabs.
2. Click **Secure Server Wizard**. The first screen of the wizard opens, as shown in Figure 5-45.

*Figure 5-45 Starting the Secure Server Wizard*



3. Follow the instructions and prompts in the wizard to configure the secure server. When you have completed configuring the server, you can immediately configure another one or exit the Secure Server wizard.



# FIPS Operation

---

This chapter describes how to use the Secure Content Accelerator in FIPS Mode for FIPS 140-2-compliant operation. This chapter contains the following sections:

- FIPS Capabilities
- Using FIPS Mode
- Command Changes
- Returning to Normal Operation
- More Information

# FIPS Capabilities

The Secure Content Accelerator configuration manager is used in FIPS-Compliant Mode (“FIPS Mode”) to create and configure FIPS-compliant servers. When operating in FIPS Mode, the Secure Content Accelerator supports FIPS-compliant security. Among the FIPS-compliant features of the Secure Content Accelerator are the following:

- Only FIPS-approved algorithms are supported (DES and 3DES with SHA).
- A server using any other algorithms is disabled in FIPS Mode and cannot be used or configured.
- Only FIPS-compliant servers can be used when the device is operated in FIPS Mode. Non-FIPS 104-2-compliant servers can be configured for compliance.
- Management is available only via a serial connection.
- Passwords at least eight characters in length are required at both access and configuration levels.
- Commands that do not support FIPS-compliant security measures are disabled in FIPS Mode.
- The command prompt contains the text “[FIPS]” to indicate the device is operating in FIPS Mode.



---

**Caution**

To ensure the security of SSL sessions, you must use your own keys and certificates. The default keys and certificates preloaded on the device are intended for testing purposes only.

---

# Using FIPS Mode

FIPS Mode acts as a filtering system, allowing only FIPS Level 2-compliant SSL objects to be used for data transfer. Entering FIPS Mode is a two-step process: starting the FIPS Mode process and rebooting the device in FIPS Mode.

1. Connect to the device using a serial management session and enter Privileged Mode.

```
SCA> enable
SCA#
```

2. Enable FIPS operation.

```
SCA# fips enable
```

3. A caution is displayed. Read the text carefully before replying to it.

```
Enabling FIPS mode will cause a restart of the device.
Entering FIPS mode will also change the behavior of the device.
  Only FIPS-approved algorithms are supported.
  Only FIPS-compliant servers can be used.
  Management is available only via the serial console.
  Passwords must be at least eight characters long.
  Firmware signature verification is enabled.
  Some commands are not supported.
Are you sure you want to do this? (y/n) [n]
```

4. The Secure Content Accelerator checks access- and enable-level passwords previously set, if any. The display reflects the state of current passwords:



---

**Note** FIPS Mode passwords must be at least eight characters in length and are limited to a character set containing the alphabet, Arabic numerals, period (.), hyphen (-), underscore (\_), and !@#%&\*+=[ ] { } ; : < > ? ~ .

---

- a. If no passwords had been set previously, this text is displayed:

```
You need to provide an access-level password of at least 8
characters.
Enter new password:
Confirm password:
You need to provide an enable-level password of at least 8
characters.
Enter new password:
Confirm new password:
```



**Note**

---

Passwords are not echoed to the screen. These passwords are not FIPS-specific and are prompted for when the device is used in normal operation.

---

- b. If the previously set access-level password is not appropriate for FIPS Mode operation, the following text is displayed:

```
Your current access-level password is not valid for FIPS mode.
You need to provide an access-level password of at least 8
characters.
Enter new password:
Confirm password:
```

- c. If the previously set enable-level password is not appropriate for FIPS Mode operation, the following text is displayed:

```
Your current enable-level password is not valid for FIPS mode.
You need to provide an access-level password of at least 8
characters.
Enter new password:
Confirm password:
```

- d. If both the previously set access- and enable-level passwords are valid for FIPS Mode operation, no additional text is displayed.
5. The device reboots and enters FIPS Mode. Enter the access-level password to control the device.

```
Enter the access-level password:
```



**Caution**

If you cannot remember the passwords, you will not be able to view device status and statistics or configure the device. The only option is to use the “FailSafe” password as described in “Factory Default Reset Password” section on page 4-4. **All configuration will be lost!**

6. Use the enable-level password to enter Privileged Mode.

Enter the enable-level password:

## Creating a Server in FIPS Mode

Creating and configuring server operations in FIPS Mode are nearly identical to those in normal operational modes. The differences are the following:

- Only the FIPS security policy and security policies containing FIPS-approved algorithms can be used
- Only FIPS-compliant servers can be used for data transfer (non-FIPS-compliant servers can be edited for FIPS compliance)

Follow the steps below to create a FIPS-compliant server.

1. Connect to the Secure Content Accelerator using a serial management session, and enter Privileged, Configuration, and SSL Modes. Create a secure server named *mySecServ*.

```
[FIPS] SCA> enable
[FIPS] SCA# config
[FIPS] config[SCA]# ssl
[FIPS] ssl-config[SCA]# server mySecServ create
[FIPS] ssl-server[mySecServ]#>
```

2. Assign an IP address, key, certificate, and FIPS-compliant security policy.

```
[FIPS] ssl-server[mySecServ]#> ip address 10.1.114.30
[FIPS] ssl-server[mySecServ]#> key myOwnKey
[FIPS] ssl-server[mySecServ]#> cert myOwnCert
[FIPS] ssl-server[mySecServ]#> secpolicy fips
[FIPS] ssl-server[mySecServ]#>
```

3. Exit to Top Level Mode.

```
[FIPS] ssl-server[mySecServ]#> finished
[FIPS] SCA#
```

You can create a security policy containing only the FIPS-approved algorithm you want to use. The following example demonstrates creating a security policy containing on the 3DES/SHA algorithm and editing a secure server to use the new user-defined security policy rather than the FIPS security policy.

1. Connect to the Secure Content Accelerator using a serial management session, and enter Privileged, Configuration, and SSL Modes. Create a security policy named *myFIPS*.

```
[FIPS] SCA> enable
[FIPS] SCA# config
[FIPS] config[SCA]# ssl
[FIPS] ssl-config[SCA]# secpolicy myFIPS create
[FIPS] ssl-secpolicy[myFIPS]#>
```

2. Specify the 3DES/SHA cryptographic algorithm, and return to SSL Configuration Mode.

```
[FIPS] ssl-secpolicy[myFIPS]#> crypto DES-CBC3-SHA
[FIPS] ssl-secpolicy[myFIPS]#> exit
[FIPS] ssl-config[SCA]#>
```

3. Enter Server Configuration Mode to edit the configuration of the server *mySecServ* to use the *myFIPS* security policy rather than the previously specified FIPS security policy.

```
[FIPS] ssl-config[SCA]#> server mySecServ
[FIPS] ssl-server[mySecServ]#> secpolicy myFIPS
[FIPS] ssl-server[mySecServ]#>
```

4. Exit to Top Level Mode.

```
[FIPS] ssl-server[mySecServ]# finished
[FIPS] SCA#
```

# Command Changes

When the device is operated in FIPS Mode, some commands are unavailable or behave differently than in normal operating modes.

## Unavailable Commands

Commands are unavailable in FIPS Mode are shown in Table 6-1, below.

*Table 6-1 Commands Unavailable in FIPS Mode*

Operational Mode	Command
Top Level Mode	<b>attach, attach ip, discover, group, show device list, show group, show profile, show remote-management, show telnet, show web-mgmt, write file</b>
Group Configuration Mode	Group Configuration Mode is unavailable.
Configuration Mode	<b>remote-management access-list, remote-management enable, remote-management encryption, remote-management port, remote-management shared-secret, telnet access-list, telnet enable, telnet port, web-mgmt access-list, web-mgmt enable, web-mgmt port</b>

## Differing Command Behaviors

Some commands behave differently while the Secure Content Accelerator is in FIPS Mode. These commands and notes about their usage are presented in Table 6-2, below.

Table 6-2 FIPS Mode Command Changes

Mode	Command	Notes
Top Level Mode	<b>show device</b>	Settings are not displayed for telnet, remote access, and Web management. The device type area indicates the Secure Content Accelerator is in FIPS Mode.  When the Secure Content Accelerator is removed from FIPS Mode, all settings existing before entering FIPS Mode are retained with the exception of changes made while in FIPS Mode.
	<b>show ssl</b>	SSL information includes objects that are not FIPS-compliant, such as security policies other than FIPS or those containing non-FIPS-compliant algorithms.
	<b>show ssl secpolicy</b>	Information can be shown for individual, non-FIPS-compliant security policies.
	<b>show ssl server</b>	Information can be shown for all servers. All non-FIPS-compliant servers are disabled by default in FIPS Mode and cannot be enabled.
	<b>quick-start</b>	When using the QuickStart wizard to create a server, only the FIPS security policy is available. When using the QuickStart wizard to configure an existing server, only FIPS-compliant servers can be configured and only the FIPS security policy is available.
Configuration Mode	<b>access-list</b>	You can create access lists while in FIPS Mode. However, because remote, telnet, and GUI management methods are unavailable in FIPS Mode, the access lists assigned to those subsystems cannot be used. These access lists are available when the device is returned to normal operation. Access lists can be assigned to the SNMP subsystem while in FIPS Mode.
	<b>password</b>	FIPS Mode passwords must be at least eight characters in length and are limited to a character set containing the alphabet, Arabic numerals, period (.), hyphen (-), underscore (_), and !@#\$%^&*+=[ ] { } ; : < > ? ~ .

Table 6-2 FIPS Mode Command Changes (continued)

Mode	Command	Notes
Backend Server Configuration Mode	<b>secpolicy</b>	You can only assign the FIPS security policy or a user-defined security policy containing FIPS-approved algorithms. The completer for this command lists only security policies with FIPS-approved algorithms.
Reverse-Proxy Server Configuration Mode	<b>secpolicy</b>	You can only assign the FIPS security policy or a user-defined security policy containing FIPS-approved algorithms. The completer for this command lists only security policies with FIPS-approved algorithms.
Security Policy Configuration Mode	<b>crypto</b>	You can create only security policies containing FIPS-approved algorithms: DES-CBC-SHA and/or DES-CBC3-SHA.
Server Configuration Mode	<b>secpolicy</b>	You can only assign the FIPS security policy or a user-defined security policy containing FIPS-approved algorithms. The completer for this command lists only security policies with FIPS-approved algorithms.

## Returning to Normal Operation

Follow these steps to return the Secure Content Accelerator to normal operation.

1. Connect to the device using a serial management session and enter Privileged Mode.

```
[FIPS] SCA> enable
[FIPS] SCA#
```

2. Disable FIPS operation.

```
[FIPS] SCA# no fips enable
```

3. Press **y** when prompted to reboot the Secure Content Accelerator. After the device reboots, you are prompted for the access-level password. When the password is accepted, the “[FIPS]” portion of the prompt is removed, reflecting normal operation of the Secure Content Accelerator.

# More Information

For more information about the NIST Cryptographic Module Validation Program, see <http://csrc.nist.gov/cryptval/cmvp.htm>.



# Specifications

---

This appendix presents the specifications for both Secure Content Accelerator versions. It contains the following sections:

- Electrical Specifications
- Environmental Specifications
- Physical Specifications

# Electrical Specifications

Table A-1 describes the Secure Content Accelerator electrical specifications.

*Table A-1 AC Electrical Specifications*

DC Specification	Secure Content Accelerator
Voltage AC	100-240 VAC, 50-60 Hz
Current Consumption (maximum)	0.5 A



## Warning

The device is designed to work with TN power systems. This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

# Environmental Specifications

Table A-2 describes the Secure Content Accelerator environmental specifications.

*Table A-2 Environmental Specifications*

Specification	Secure Content Accelerator
Ambient Operating Temperature (maximum)	41°-105° F (5°-40° C)



# Physical Specifications

Table A-3 describes the Secure Content Accelerator physical specifications.

**Table A-3** *Physical Specifications*

Specification	Secure Content Accelerator
Chassis Dimensions (H x W x D)	10x1.75x17 inches (25x4.4x42.5 cm)
Shipping Weight	6 lbs (2.72 kg)





## Deployment Examples

---

The following examples demonstrate how the Secure Content Accelerator can be integrated into a network.

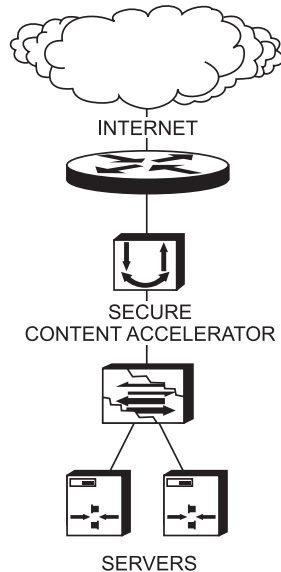
This appendix contains the following sections:

- Single Device
- Load Balancing
- Use with the CSS
- Connecting the Device to a Terminal Server
- Web Site Changes

# Single Device

A single Secure Content Accelerator provides SSL offloading and processing for an entire server farm, as shown in Figure B-1.

*Figure B-1 Single Secure Content Accelerator Installation*

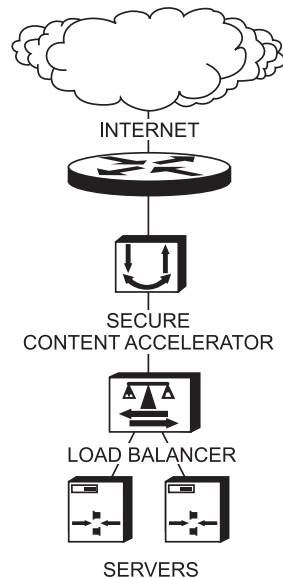


1. Install the appliance as instructed previously.
2. Connect the “Network” Ethernet interface to the Internet.
3. Connect the “Server” Ethernet interface to Web server access.

## Load Balancing

Secure Content Accelerator devices can be installed in front of or behind a load balancer. If the load balancer is using URL- or cookie-related load balancing, install the appliance in front of the load balancer. In this configuration, the load balancer receives clear text packets decrypted by the SSL device. Figure B-2 shows a typical installation.

**Figure B-2** Secure Content Accelerator Installation with a Load Balancer



1. Install the appliance as instructed previously.
2. Connect the “Network” Ethernet interface to the Internet. Connect the “Server” Ethernet interface to the load balancer.

For information about configuring the Secure Content Accelerator in conjunction with the CSS 11000 Series Content Services Switch (hereinafter referred to as the CSS), see “Use with the CSS”.

## Use with the CSS

Using the Secure Content Accelerator with the CSS allows Layer 4 load balancing of the Secure Content Accelerator and Layer 5 routing and load balancing for content decrypted by the Secure Content Accelerator. Four deployment scenarios are recommended:

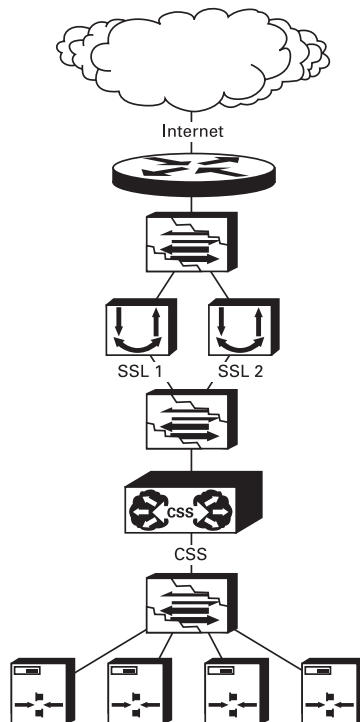
- In-Line
- Transparent Sandwich

- One-Armed Non-Transparent Proxy
- One-Armed Transparent Proxy

## In-Line

Placing the Secure Content Accelerator in front of the CSS increases performance of the server farm by offloading all SSL processing from the servers. The Secure Content Accelerator is completely transparent to the CSS and servers.

This deployment is the simplest to configure because it requires no specific inter-operational configuration on either the Secure Content Accelerator or the CSS. However, the deployment provides a low level of scalability, based upon the capacity of the CSS. An example deployment is shown in Figure B-3.

**Figure B-3 Secure Content Accelerator In-Line Installation**

The CSS is used to front-end one or more Secure Content Accelerator devices. Because the Secure Content Accelerator is a Layer 2 device, it must be configured to ensure that bridge loops are not created. If multiple Secure Content Accelerator devices are used, each must be attached to a separate VLAN on the CSS and/or the upstream Layer 2 switch. The Secure Content Accelerator intercepts all port 443 traffic for the IP addresses configured on it, decrypts the traffic, and forwards it as clear text on another TCP service port to the CSS. All port 80 traffic is bridged transparently to the CSS. Table B-1 shows basic configuration actions for both the CSS and Secure Content Accelerator.

**Table B-1 In-Line Installation Device Configuration**

CSS Configuration	Secure Content Accelerator Configuration
<ul style="list-style-type: none"> <li>• Create a VLAN for each Secure Content Accelerator</li> <li>• Create a VLAN for the servers</li> <li>• Create services as required for each server, adding “keepalive” attributes as necessary</li> <li>• Create a default ECMP route for each load balanced Secure Content Accelerator using the upstream router as the gateway for each upstream VLAN</li> <li>• Create Layer 5 rules for the secure content</li> <li>• Create content rules as required for non-secure content</li> </ul>	<ul style="list-style-type: none"> <li>• Export keys and certificates from any existing secure servers, if necessary</li> <li>• Assign an IP address to each Secure Content Accelerator as specified in the CSS configuration</li> <li>• Assign a default route for each Secure Content Accelerator using the CSS VLAN circuit IP address as the gateway</li> <li>• Set up one or more logical secure servers using QuickStart wizard (Chapter 3) or configuration manager (Chapter 4)</li> </ul>

The following listing shows a sample configuration for the CSS.

```
!Generated on 11/18/2000 11:01:18
!Active version: ap0400007s

configure

!***** GLOBAL *****
  bridge spanning-tree disabled
  no restrict web-mgmt

  ip route 0.0.0.0 0.0.0.0 10.176.11.1 1

!***** INTERFACE *****
interface ethernet-8
  bridge vlan 8

!***** CIRCUIT *****
circuit VLAN1
  ip address 10.176.10.1 255.255.255.0

circuit VLAN8
  ip address 10.176.11.2 255.255.255.0
```



```
!***** SERVICE *****
service s1
  ip address 10.176.10.10
  protocol tcp
  active

service s2
  ip address 10.176.10.11
  protocol tcp
  active

service s3
  ip address 10.176.10.12
  protocol tcp
  active

service s4
  ip address 10.176.10.13
  protocol tcp
  active

!***** OWNER *****
owner test

content http-non-secure-port-80
  vip address 10.176.11.100
  protocol tcp
  port 80
  url "/"
  add service s1
  add service s2
  add service s3
  add service s4
  active

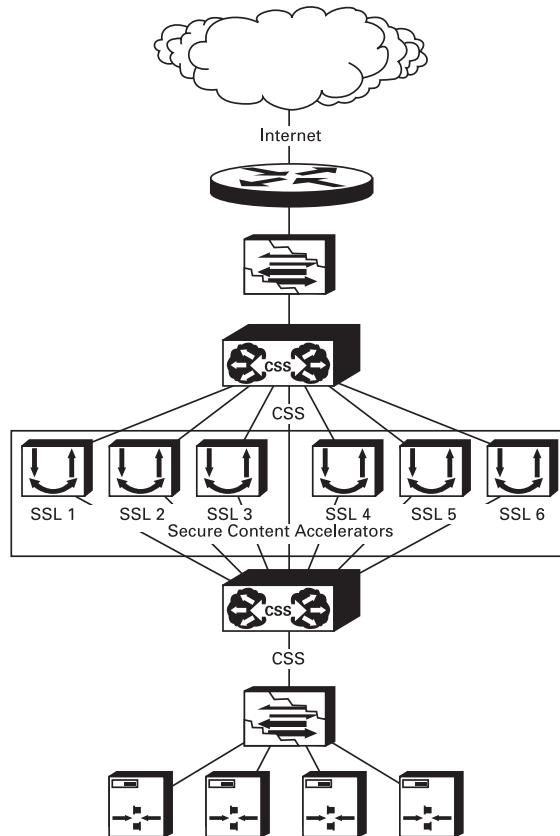
content http-secure-port-81
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 81
  url "/secure/"
  active
```

## Transparent Sandwich

This deployment places one or more Secure Content Accelerator devices between two CSS devices, allowing load balancing of up to 15 Secure Content Accelerator devices. Applications such as reverse proxy caching and content type separation can be enabled.

The transparent sandwich deployment is moderately difficult to configure with good scalability. A minimum of two CSS devices are required. Figure B-4 shows a typical deployment.

**Figure B-4** Secure Content Accelerator Transparent Sandwich Installation



The upstream CSS is configured as if the Secure Content Accelerator devices are transparent caches with redirection at Layer 4. Port 80 traffic is forwarded via Layer 3 to the downstream CSS, avoiding any potential Port 80 bottleneck at the Secure Content Accelerator level. Because the Secure Content Accelerator is a Layer 2 device, it must be configured to ensure that bridge loops are not created.

The Secure Content Accelerator intercepts all port 443 traffic for the IP addresses configured on it, decrypts the traffic, and forwards it as clear text on another TCP service port to the downstream CSS. The downstream CSS is configured with Layer 5 rules for all origin servers and multiple ECMP routes, each to a different upstream VLAN. The default ECMP configuration is to prefer ingress, ensuring that outbound traffic needing to be encrypted is routed to the Secure Content Accelerator responsible for decrypting traffic for that session. Outbound Port 80 traffic bypasses the Secure Content Accelerator devices completely.

Traffic “sourced” from a server in the server farm can be routed through one of the Secure Content Accelerator devices. There is no way to differentiate between equal cost paths without mapping to an ingress flow. Table B-2 shows basic configuration actions for the CSS devices and Secure Content Accelerator.

**Table B-2** *Transparent Sandwich Installation Device Configuration*

Upstream CSS Configuration	Secure Content Accelerator Configuration	Downstream CSS Configuration
<ul style="list-style-type: none"> <li>• Create a VLAN for each Secure Content Accelerator to be load balanced</li> <li>• Create a separate VLAN to connect to the downstream CSS to route port 80 traffic directly</li> <li>• Create a service for each Secure Content Accelerator with the IP address of the corresponding circuit address on the downstream Secure Content Accelerator; define the services as type “transparent-cache”</li> <li>• Create a Layer 4 content rule to balance the Secure Content Accelerators, using advanced-balance ssl and application ssl to assist SSL v.3 key reuse, in one of the following ways: <ul style="list-style-type: none"> <li>– Without a VIP: if you do not specify a VIP, all port 443 traffic is forwarded to the Secure Content Accelerators</li> <li>– With a VIP: when you specify a VIP, any port 443 traffic not destined to that VIP can be routed over the VLAN specified for port 80 and SSL traffic terminated on origin servers</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Export keys and certificates from any existing secure servers, if necessary</li> <li>• Assign an IP address to each Secure Content Accelerator as specified in the CSS configuration</li> <li>• Assign a default route for each Secure Content Accelerator using the upstream CS VLAN circuit IP address as the gateway</li> <li>• Set up one or more logical secure servers using QuickStart wizard (Chapter 3) or configuration manager (Chapter 4); you may wish to use TCP service port 81 as the <b>remoteport</b></li> <li>• Assign a static route for the VIP to point to the downstream CSS VLAN circuit IP address</li> </ul>	<ul style="list-style-type: none"> <li>• Create a VLAN for each Secure Content Accelerator</li> <li>• Create a VLAN to connect to the upstream CSS to route port 80 traffic directly</li> <li>• Create services as required for each server, adding “keepalive” attributes as necessary</li> <li>• Create a default ECMP route for each load balanced Secure Content Accelerator using the upstream router as the gateway for each upstream VLAN</li> <li>• Create a default route to the upstream CSS to allow non-SSL traffic to bypass the Secure Content Accelerator</li> <li>• Create Layer 5 rules for the secure content</li> <li>• Create content rules as required for non-secure content</li> </ul>

The following is a sample configuration for the upstream CSS.

```
!Generated on 11/18/2000 11:03:28
!Active version: ap0400007s

configure

!***** GLOBAL *****

  ip route 0.0.0.0 0.0.0.0 10.100.1.1 1
  ip route 10.176.10.0 255.255.255.0 10.176.11.0

!***** INTERFACE *****
interface ethernet-2
  bridge vlan 2

interface ethernet-3
  bridge vlan 3

interface ethernet-4
  bridge vlan 4

interface ethernet-5
  bridge vlan 5

interface ethernet-6
  bridge vlan 6

interface ethernet-7
  bridge vlan 7

interface ethernet-8
  bridge vlan 8

!***** CIRCUIT *****
circuit VLAN1

  ip address 10.176.1.1 255.255.255.0

circuit VLAN2

  ip address 10.176.2.1 255.255.255.0

circuit VLAN3

  ip address 10.176.3.1 255.255.255.0
```

```
circuit VLAN4
    ip address 10.176.4.1 255.255.255.0

circuit VLAN5
    ip address 10.176.5.1 255.255.255.0

circuit VLAN6
    ip address 10.176.6.1 255.255.255.0

circuit VLAN7
    ip address 10.176.11.1 255.255.255.0

circuit VLAN8
    ip address 10.100.132.101 255.255.0.0

!***** SERVICE *****
service ssl1
    port 443
    protocol tcp
    ip address 10.176.1.3
    type transparent-cache
    active

service ssl2
    port 443
    protocol tcp
    ip address 10.176.2.3
    type transparent-cache
    active

service ssl3
    port 443
    protocol tcp
    ip address 10.176.3.3
    type transparent-cache
    active

service ssl4
    port 443
    protocol tcp
    ip address 10.176.4.3
    type transparent-cache
    active
```

```
service ssl5
  port 443
  protocol tcp
  ip address 10.176.5.3
  type transparent-cache
  active

service ssl6
  port 443
  protocol tcp
  ip address 10.176.6.3
  type transparent-cache
  active

!***** OWNER *****
owner test

content ssl
  protocol tcp
  port 443
  add service ssl1
  add service ssl2
  add service ssl3
  add service ssl4
  add service ssl5
  add service ssl6
  active
```

The following is a sample configuration for the downstream CSS.

```

!Generated on 11/18/2000 11:01:18
!Active version: ap0400007s

configure

!***** GLOBAL *****
  bridge spanning-tree disabled
  no restrict web-mgmt

  ip route 0.0.0.0 0.0.0.0 10.176.1.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.2.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.3.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.4.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.5.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.6.1 1
  ip route 0.0.0.0 0.0.0.0 10.176.11.1 1

!***** INTERFACE *****
interface ethernet-2
  bridge vlan 2

interface ethernet-3
  bridge vlan 3

interface ethernet-4
  bridge vlan 4

interface ethernet-5
  bridge vlan 5

interface ethernet-6
  bridge vlan 6

interface ethernet-7
  bridge vlan 7

interface ethernet-8
  bridge vlan 8

!***** CIRCUIT *****
circuit VLAN2

  ip address 10.176.2.3 255.255.255.0

circuit VLAN3

  ip address 10.176.3.3 255.255.255.0

```



```
circuit VLAN4
    ip address 10.176.4.3 255.255.255.0

circuit VLAN5
    ip address 10.176.5.3 255.255.255.0

circuit VLAN6
    ip address 10.176.6.3 255.255.255.0

circuit VLAN7
    ip address 10.176.10.1 255.255.255.0

circuit VLAN8
    ip address 10.176.11.2 255.255.255.0

circuit VLAN1
    ip address 10.176.1.3 255.255.255.0

!***** SERVICE *****
service s1
    ip address 10.176.10.10
    protocol tcp
    active

service s2
    ip address 10.176.10.11
    protocol tcp
    active

service s3
    ip address 10.176.10.12
    protocol tcp
    active

service s4
    ip address 10.176.10.13
    protocol tcp
    active
```

```

!***** OWNER *****
owner test

content http-non-secure-port-80
  vip address 10.176.11.100
  protocol tcp
  port 80
  url "/*"
  add service s1
  add service s2
  add service s3
  add service s4
  active

content http-secure-port-81
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 81
  url "/secure/*"
  active

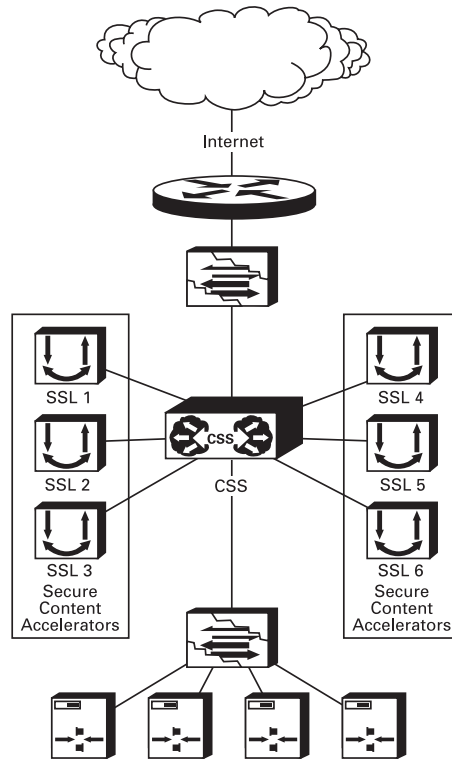
```

## One-Armed Non-Transparent Proxy

This deployment uses a single CSS for load balancing SSL offloading and Layer 5 switching, allowing load balancing at up to the limit of transactions per second of the CSS. Applications such as reverse proxy caching and content type separation can be enabled. The level depends upon the type of content and the mix of HTTP 1.0 and HTTP 1.1 traffic.

The one-armed non-transparent proxy deployment is complex to configure, but it provides a high degree of scalability. If IP address accounting is required, use the command **log-url** when configuring the Secure Content Accelerator. This command instructs the device to write a client access log to a specific host. The resulting log file can be utilized by all popular log analysis tools. Figure B-5 shows a typical deployment.

**Figure B-5 Secure Content Accelerator One-Armed Non-Transparent Proxy Installation**



In this deployment the CSS is configured with both Layer 4 and Layer 5 rules. For each VIP configured on the CSS for services terminating on the Secure Content Accelerator, a service must be defined for the Secure Content Accelerator devices, each with a different destination port definition.

The Secure Content Accelerator does not use the IP address to ensure traffic is sent to the correct server because the CSS changes the destination IP address to that of the Secure Content Accelerator. The Secure Content Accelerator is configured only at Layer 4. This configuration requires setting multiple destination IP/destination port pairs on the Secure Content Accelerator. Bridge loops are not created because all port 443 traffic terminates on Secure Content Accelerator devices each connected to the CSS via a single port. Table B-3 shows basic configuration actions for both the CSS and Secure Content Accelerator.

**Table B-3 One-Armed Non-Transparent Proxy Installation Device Configuration**

CSS Configuration	Secure Content Accelerator Configuration
<ul style="list-style-type: none"> <li>• Create a VLAN for the upstream router</li> <li>• Create one VLAN for all connected Secure Content Accelerator devices</li> <li>• Create a separate VLAN for the servers</li> <li>• Create a service for each Secure Content Accelerator IP address and destination port pair</li> <li>• Create services as required for each server (adding “keepalive” attributes as necessary)</li> <li>• Create a default route to the upstream router</li> <li>• Create Layer 4 rules for each incoming VIP and add appropriate Secure Content Accelerator services</li> <li>• Create Layer 5 rules for the secure content</li> <li>• Create content rules as required for non-secure content</li> </ul>	<ul style="list-style-type: none"> <li>• Export keys and certificates from any existing secure servers, if necessary</li> <li>• Assign an IP address to each Secure Content Accelerator as specified in the CSS configuration</li> <li>• Assign a default route for each Secure Content Accelerator using the CSS VLAN circuit IP address as the gateway</li> <li>• Set up one or more logical secure servers using the QuickStart wizard (Chapter 3) or configuration manager (Chapter 4)</li> <li>• Set up single-port operation using the <b>mode one-port</b> command (Appendix C)</li> <li>• If client IP accounting is necessary, use the <b>log-url</b> command to specify the host for writing the access log</li> </ul>

Below is a sample configuration for the CSS.

```
!Generated on 11/18/2000 17:38:37
!Active version: ap0400007s

configure

!***** GLOBAL *****
bridge spanning-tree disabled

ip route 0.0.0.0 0.0.0.0 10.100.1.1 1
```

```
!***** INTERFACE *****
interface ethernet-7
  bridge vlan 7

interface ethernet-8
  bridge vlan 8

!***** CIRCUIT *****
circuit VLAN1

  ip address 10.176.1.1 255.255.255.0

circuit VLAN7

  ip address 10.176.10.1 255.255.255.0

circuit VLAN8

  ip address 10.100.132.101 255.255.0.0

!***** SERVICE *****
service s1
  ip address 10.176.10.10
  protocol tcp
  active

service s2
  ip address 10.176.10.11
  protocol tcp
  active

service s3
  ip address 10.176.10.12
  protocol tcp
  active

service s4
  ip address 10.176.10.13
  protocol tcp
  active

service ssl1-443
  port 443
  protocol tcp
  ip address 10.176.1.3
  active
```

```
service ssl1-444
  ip address 10.176.1.3
  protocol tcp
  port 444
  active
```

```
service ssl2-443
  port 443
  protocol tcp
  ip address 10.176.1.4
  active
```

```
service ssl2-444
  port 444
  protocol tcp
  ip address 10.176.1.4
  active
```

```
service ssl3-443
  port 443
  protocol tcp
  ip address 10.176.1.5
  active
```

```
service ssl3-444
  port 444
  protocol tcp
  ip address 10.176.1.5
  active
```

```
service ssl4-443
  port 443
  protocol tcp
  ip address 10.176.1.6
  active
```

```
service ssl4-444
  port 444
  protocol tcp
  ip address 10.176.1.6
  active
```

```
service ssl5-443
  port 443
  protocol tcp
  ip address 10.176.1.7
  active
```

```
service ssl5-444
  port 444
  protocol tcp
  ip address 10.176.1.7
  active

service ssl6-443
  port 443
  protocol tcp
  ip address 10.176.1.8
  active

service ssl6-444
  port 444
  protocol tcp
  ip address 10.176.1.8
  active

!***** OWNER *****
owner test

content http-secure-port-81
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 81
  url "/secure/*"
  active

content http-non-secure-port-80
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 81
  url "/*"
  active

content ssl
  vip address 10.176.11.100
  protocol tcp
  port 443
  add service ssl1-443
```

```
add service ssl2-443
add service ssl3-443
add service ssl4-443
add service ssl5-443
add service ssl6-443
active

content ssl-444
protocol tcp
vip address 10.176.11.101
port 443
add service ssl2-444
add service ssl11-444
add service ssl3-444
add service ssl4-444
add service ssl5-444
add service ssl6-444
active
```

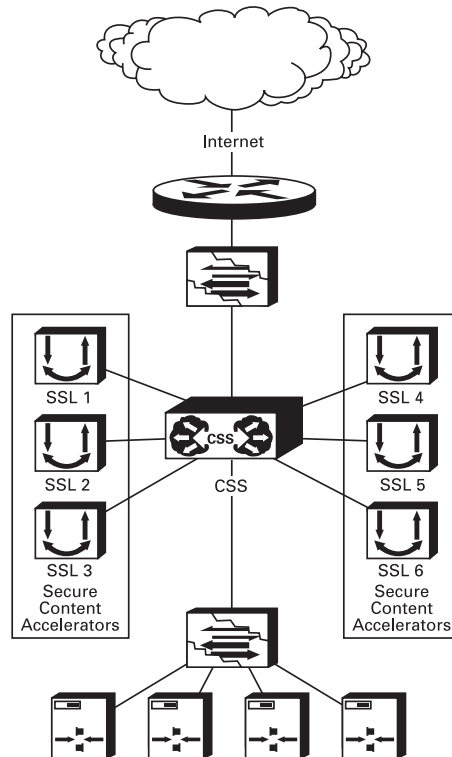
## One-Armed Transparent Proxy

This deployment uses a single CSS for load balancing up to 15 Secure Content Accelerator devices. The deployment combines the single CSS solution of the proxy deployment with the transparency of the sandwich deployment.

The one-armed transparent proxy deployment is the most complex to configure, but it provides a high degree of scalability and extended features, including IP address accounting. Figure B-6 shows a typical deployment.



**Figure B-6 Secure Content Accelerator One-Armed Transparent Proxy Installation**



This deployment has several constraints:

- No SSL client can be attached to a directly connected subnet; all SSL clients must pass through an upstream router.
- ACLs must be written so that Secure Content Accelerator management and other applications are passed through the CSS properly.
- Static routes must be added to the CSS so that traffic that should not pass through the Secure Content Accelerator devices is routed properly.

**Caution**

---

ACLs and static routes must be configured carefully. If a device or network is specified in an ACL or static route in such a way that it will force all traffic to the upstream router's ECMP route, all traffic matching the ACL or static route will bypass the Secure Content Accelerator devices. Thus management of the Secure Content Accelerator devices and management stations requiring ICMP or SNMP to operate will not have access to SSL processing.

---

Table B-4 shows basic configuration actions for both the CSS and Secure Content Accelerator.

**Table B-4 One-Armed Transparent Proxy Installation Device Configuration**

CSS Configuration	Secure Content Accelerator Configuration
<ul style="list-style-type: none"> <li>• Create a VLAN for each Secure Content Accelerator to be load balanced</li> <li>• Create a VLAN for the upstream router</li> <li>• Create a separate VLAN for the servers</li> <li>• Create a default route with the upstream router as the gateway</li> <li>• Create a default route with each Secure Content Accelerator as a gateway</li> <li>• Define a static route for each management workstation not connected to a directly attached subnet</li> <li>• Define a service for each Secure Content Accelerator with its IP address, ensuring that the type is “transparent” and that “no cache-bypass” is configured</li> <li>• Create services as required for each server (adding “keepalive” attributes as necessary)</li> <li>• Create Layer 4 content rules to balance the Secure Content Accelerator devices; you may use “advanced-balance ssl” and “application ssl” to assist with SSL V.3 key reuse</li> <li>• Create Layer 5 rules for secure content</li> <li>• Create content rules as required for non-secure content</li> <li>• Define ACLs and upstream router service to ensure proper routing of traffic not terminated on the CSS</li> </ul>	<ul style="list-style-type: none"> <li>• Export keys and certificates from any existing secure servers, if necessary</li> <li>• Assign an IP address to each Secure Content Accelerator as specified in the CSS configuration</li> <li>• Assign a default route for each Secure Content Accelerator using the CSS VLAN circuit IP address as the gateway</li> <li>• Set up one or more logical secure servers using QuickStart wizard (Chapter 3) or configuration manager (Chapter 4)</li> <li>• Set up single-port operation using the <b>mode one-port</b> command (Appendix C)</li> </ul>

Below is a sample configuration for the CSS.

```

!Generated on 11/28/2000 16:15:49
!Active version: ap0400007s

configure

!***** GLOBAL *****

acl enable

ip route 0.0.0.0 0.0.0.0 10.176.50.1 1
ip route 0.0.0.0 0.0.0.0 10.176.1.3 1
ip route 0.0.0.0 0.0.0.0 10.176.2.3 1
ip route 0.0.0.0 0.0.0.0 10.176.3.3 1
ip route 0.0.0.0 0.0.0.0 10.176.4.3 1
ip route 0.0.0.0 0.0.0.0 10.176.5.3 1
ip route 0.0.0.0 0.0.0.0 10.176.6.3 1
! network management station static route
ip route 10.176.50.100 255.255.255.255 10.176.50.1 1

!***** INTERFACE *****

interface ethernet-2
  bridge vlan 2

interface ethernet-3
  bridge vlan 3

interface ethernet-4
  bridge vlan 4

interface ethernet-5
  bridge vlan 5

interface ethernet-6
  bridge vlan 6

interface ethernet-7
  bridge vlan 7

interface ethernet-8
  bridge vlan 8

!***** CIRCUIT *****

circuit VLAN1

  ip address 10.176.1.1 255.255.255.0

```

```
circuit VLAN2

    ip address 10.176.2.1 255.255.255.0

circuit VLAN3

    ip address 10.176.3.1 255.255.255.0

circuit VLAN4

    ip address 10.176.4.1 255.255.255.0

circuit VLAN5

    ip address 10.176.5.1 255.255.255.0

circuit VLAN6

    ip address 10.176.6.1 255.255.255.0

circuit VLAN7

    ip address 10.176.10.1 255.255.255.0

circuit VLAN8

    ip address 10.176.50.2 255.255.255.0

!***** SERVICE *****
service s1
    ip address 10.176.10.10
    protocol tcp
    active

service s2
    ip address 10.176.10.11
    protocol tcp
    active

service s3
    ip address 10.176.10.12
    protocol tcp
    active

service s4
    ip address 10.176.10.13
    protocol tcp
    active
```

```
service ssl1
  port 443
  protocol tcp
  ip address 10.176.1.3
  type transparent-cache
  no cache-bypass
  active

service ssl2
  port 443
  protocol tcp
  type transparent-cache
  no cache-bypass
  ip address 10.176.2.3
  active

service ssl3
  port 443
  protocol tcp
  type transparent-cache
  no cache-bypass
  ip address 10.176.3.3
  active

service ssl4
  port 443
  protocol tcp
  type transparent-cache
  no cache-bypass
  ip address 10.176.4.3
  active

service ssl5
  port 443
  protocol tcp
  type transparent-cache
  no cache-bypass
  ip address 10.176.5.3
  active

service ssl6
  port 443
  protocol tcp
  type transparent-cache
  no cache-bypass
  ip address 10.176.6.3
  active
```

```
service upstream-router
  ip address 10.176.50.1
  type transparent-cache
  active

!***** OWNER *****
owner test

content http-secure-port-81
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 81
  url "/secure/*"
  active

content http-non-secure-port-80
  vip address 10.176.11.100
  add service s1
  add service s2
  add service s3
  add service s4
  protocol tcp
  port 80
  url "/*"
  active

content ssl
  protocol tcp
  port 443
  add service ssl1
  add service ssl2
  add service ssl3
  add service ssl4
  add service ssl5
  add service ssl6
  vip address 10.176.11.100
  active

!***** ACL *****
acl 8
  clause 10 permit any any destination any
  apply circuit-(VLAN8)
```

```

acl 7
  clause 10 permit any any destination any
  apply circuit-(VLAN7)

acl 6
  clause 10 permit any any destination any eq 443
  clause 20 permit any any destination any eq 81
  clause 30 permit tcp any destination any eq 2932
  clause 40 permit udp any destination any eq 2932
  clause 50 permit udp any eq 2932 destination any prefer
upstream-router
  clause 99 permit any any destination any
  apply circuit-(VLAN6)
  apply circuit-(VLAN5)
  apply circuit-(VLAN4)
  apply circuit-(VLAN3)
  apply circuit-(VLAN2)
  apply circuit-(VLAN1)

```

## Connecting the Device to a Terminal Server

The Secure Content Accelerator can be connected to a terminal server, such as the Cisco 2511 Access Server. You will need a standard RJ45-DB9F adapter (CAB-9AS-FDTE, part number 74-0495-01).

1. Attach the RJ45-DB9F adapter to the CONSOLE port of the Secure Content Accelerator.
2. Using an octal cable with RJ45 connectors, attach the terminal server to the Secure Content Accelerator via the RJ45-DB9F adapter.
3. Using the line interface on the terminal server, use these commands:

```

line 1
  autocommand connect
  transport input all

```



### Note

If you are using firmware older than 3.0.5 on the Secure Content Accelerator, also use the command **speed 115200**.



# Web Site Changes

You must make changes to your existing Web pages before users can access them.

1. Install and configure the Secure Content Accelerator.
2. Create a non-secure (“http://”-prefixed) Web page as an entry point for the Web site. Include some method of transferring the user to the secure (“https://”-prefixed) URL. You may use a button, hypertext link, image map, automatic redirection, or any other method you choose.
3. If your site does not use relative links, change the “http://” portion of every link (including graphic links) to “https://”; otherwise, links should remain the same.



---

**Note**

If you are using IIS and have a redirection in your Web page, the URL must have a trailing slash (“/”) to work properly, e.g.,  
`<href=“/issamples/default/learn/”>`.

---





## Command Summary

---

This appendix contains a categorized complete listing of CLI configuration manager commands for the Secure Content Accelerator. Each command is described and, where appropriate, an example of usage is included. Some commands are available only with specific configuration connection methods. Availability of each command is indicated. Configuration using the GUI is described in Chapter 5. Configuration for FIPS-compliant operation is presented in Chapter 6, FIPS Operation.

This appendix contains the following sections:

- Input Data Format Specification
- Text Conventions
- Editing and Completion Features
- Command Hierarchy
- Configuration Security
- Methods to Manage the Device
- Initiating a Management Session
- Using the Remote Configuration Manager
- Top Level Command Set
- Group Configuration Command Set
- Configuration Command Set

# Input Data Format Specification

Table C-1 describes the data formats acceptable for most commands.

**Table C-1** *Input Data Formats*

Data	Data Format
MAC Address:	HH:HH:HH:HH:HH:HH
MAC Address:	HHHH.HHHH.HHHH
IP Address:	D.D.D.D
IP Address:	0xHHHHHHHH
Integer Values:	D
Integer Values:	0xH
Integer Range:	D-D

“H” is one or more hexadecimal digit [0-F] and “D” is one or more decimal digit.

## Text Conventions

**Bold text** indicates a command in a paragraph.

*Courier text* indicates text that appears in a command line (such as the command line interface) or is returned by the computer.

**Courier bold text** indicates commands and text you enter in a command line.

*Italic text* indicates the first occurrence of a new term, book title, and emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets (“<>”) are required information.

Items within square brackets (“[]”) are optional information.

Items separated by a vertical bar (“|”) are options. You can choose any of them.

**Note**

Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line with not returns except at the end of the complete command.

## Editing and Completion Features

You can use individual keys and control-key combinations to help you work with the Command Line Interface (CLI). Table C-2 describes the key and key combination functions.

**Table C-2 Key Reference**

Key(s)	Function
TAB	Completes the current word
?	Shows possible command completions
CTRL+A	Moves cursor to the beginning of the command line
CTRL+B	Moves cursor to the previous character
CTRL+C	Exits the QuickStart wizard at any point; the configuration is not saved
CTRL+D	When editing a command, deletes the character to the right of the cursor; otherwise, exits current configuration level or exits the configuration manager if at the Top Level
CTRL+E	Moves cursor to the end of the command line
CTRL+F	Moves cursor to the next character
CTRL+K	Erases characters from the cursor to the end of the line
CTRL+L	Clears the screen
CTRL+N	Displays the next command in the command history
CTRL+P	Displays the previous command in the command history
CTRL+U	Erases characters from the cursor to the beginning of the line
CTRL+W	Erases the previous word
CTRL+Z	Leaves current mode and returns to Top Level mode

**Table C-2 Key Reference (continued)**

Key(s)	Function
LEFT ARROW	Moves the cursor to the previous character
RIGHT ARROW	Moves the cursor to the next character
HOME	Moves cursor to the beginning of the command (not available in Solaris)
END	Moves cursor to the end of the command (not available in Solaris)

**Note**

Due to differences in operating systems, client software, and user preferences, some keys (such as ARROW, HOME, and END keys) may not work as expected. Please use the key combinations listed in the Table C-2.

Most configuration commands require completing all fields in the command. For commands that have several possible completers, the TAB or ? keys display all options.

```
SCA> show [TAB]
access-list          ip                   route
arp                  keep-alive monitor  running-configuration
copyrights           memory              snmp
cpu                  messages            ssl
device               netstat             syslog
dns                  processes           system-resources
group                profile             terminal
history              remote-management  version
interface            rip
```

The TAB key can also be used to finish a command if the command is uniquely identified by user input.

```
SCA> show cop[TAB]

results in

SCA> show copyrights
```

Additionally, commands may be abbreviated as long as the partial commands are unique. The following text:

```
SCA> sho dev lis
```

is an acceptable abbreviation for

```
SCA> show device list
```



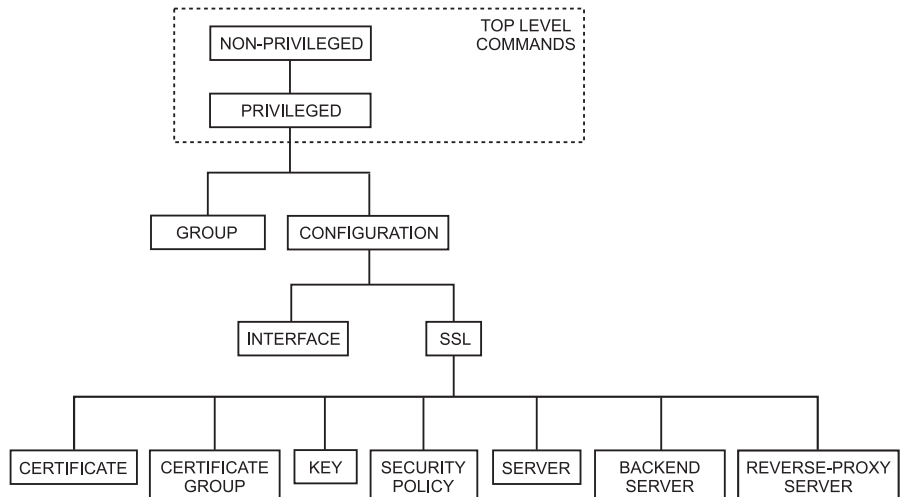
**Note**

Device, certificate, certificate group, key, security policy, and server names are case-sensitive.

## Command Hierarchy

The CLI configuration manager allows you to control hardware and SSL portions of the appliance through a discreet mode and submode system. The commands for the Secure Content Accelerator device fit into the logical hierarchy show in Figure C-1.

**Figure C-1** Command Hierarchy



To configure items in a submode, activate the submode by entering a command in the mode above it. For example, to set the network interface speed or duplex you must first enter **enable**, **configure**, then **interface network**. To return to the higher Configuration mode, simply enter **end** or **exit** or press **CTRL+D**. The **finished** command returns to the Top Level from any mode. Appendix C lists all commands for SSL devices.

## Configuration Security

Cisco Secure Content Accelerator devices allow easy, flexible configuration without compromising the security of your network or their own configuration.

### Passwords

Cisco Secure Content Accelerator devices use two levels of password protection: access- and enable-level. *Access-level passwords* control who can attach the remote configuration manager or access the device via telnet and serial connections. *Enable-level passwords* control who can view the same data available with access-level passwords as well as view sensitive data and configure the device.

SSL devices are shipped without passwords. Setting passwords is important because the device can be administered over a network. For more information about passwords, see the commands **password access** and **password enable** in Appendix C.



---

**Note**

FIPS-compliant operation requires both access- and enable-level passwords. See Chapter 6 for more information.

---



## Access Lists

Access lists control which computers can attach to a specific device. No access lists exist when you first install the Secure Content Accelerator. You can restrict the computers allowed to manage the appliance by adding their IP addresses to one or more access lists for each device. For more information about configuring access lists, see the commands **show access-list**, **access-list**, **snmp access-list**, **remote-management access-list**, **telnet access-list**, and **web-mgmt access-list** in Appendix C.



---

**Note**

In FIPS Mode you can configure access lists but can assign them only the SNMP subsystem.

---

## Encrypted Management Sessions

To further protect the configuration security, you can specify that remote (non-serial and non-telnet) configuration sessions be encrypted using AES, DES, or ARC4. See **remote-management encryption** in Appendix C.

## Factory Default Reset Password

If you have forgotten your access or enable password, you can use a factory-set password during a serial configuration session. When prompted for a password, enter *FailSafe* (case-sensitive). You are asked to confirm the action. The appliance reboots (reloads) with factory default settings.



---

**Caution**

All configuration is lost when using the factory default reset password.

---

# Methods to Manage the Device

You can configure the Cisco Secure Content Accelerator using one of four methods, three of which use the CLI configuration manager.

- Serial connection, configuration manager
  - An IP address need not have been assigned for appliance management.
  - A device can be set to single-port mode via serial connection.
  - A device must be managed while physically connected via a serial cable.
  - The FailSafe password can be used as a factory reset.
  - The only management method available in FIPS Mode.
- Telnet connection, configuration manager
  - An IP address must have been assigned to the appliance.
  - A device cannot be set to single-port mode via telnet.
  - Only one device can be managed at a time.
  - Cannot be used with Secure Content Accelerator in FIPS Mode.
- Remote network connection, configuration manager application
  - An IP address need not have been assigned for appliance management.
  - A device cannot be set to single-port mode via the remote connection.
  - Multiple devices can be attached.
  - Cannot be used with Secure Content Accelerator in FIPS Mode.
- Remote network connection, GUI
  - In IP address must have been assigned to the appliance for management.
  - A device cannot be set to single-port mode via the GUI.
  - Only one device can be managed at a single time.
  - Cannot be used with Secure Content Accelerator in FIPS Mode.

Additionally, the behaviors of some commands vary depending upon the management method. The configuration information for the commands **ip name-server**, **rdate-server**, and **ip domain-name** can be set remotely, but the configuration information is used only through a serial or telnet connection. The results of the **ping** and **traceroute** commands also are dependent upon the

management method. When used with the remote management application, these commands are executed and results returned based upon the configuring computer's hardware information. When used with serial or telnet management, the results are based upon the SSL appliance's hardware information.

Serial and telnet management commands can use symbolic hostnames in URL identifiers if the **ip domain-name** has been set.

File name formats differ depending on the management method. When using remote management, you can specify the file name as it appears in the configuring computer's file system. A path must be included, if necessary. When using serial or telnet management, the file name must be entered in any of the following formats:

```
[<http:// | ftp:// | https:// | tftp:// >] URL
```

In situations where a file is written, anonymous write access must be configured on the system with these caveats:

- http:—The server must be configured to accept PUT commands
- https:—The server must be configured to accept PUT commands
- ftp:—If anonymous write access is not allowed, use this format:  
**ftp://username:password@hostname/directory/filename**
- tftp:—Use this format:  
**tftp://hostname/filename**  
where the hostname may be either a URL or IP address

Additionally, we provide a guided QuickStart wizard configuration method, available from both the configuration manager and GUI. To use this method for configuration, see Chapter 3. Brief instructions are also included for initiating a management session using the configuration manager.

For instructions on using any of the CLI configuration managers, see Chapter 5 for instructions on using the GUI, see Chapter 6.

# Initiating a Management Session

Use the appropriate instructions below to initiate a management session with the Secure Content Accelerator.

## Serial Management and IP Address Assignment

Follow these steps to initiate a management session via a serial connection and set an IP address for the device.

**Note**

---

The default terminal settings on the SSL devices and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, please use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

---

**Note**

---

When operating in FIPS Mode, only serial management access of available.

---

1. Attach the included null modem cable to the appliance port marked “CONSOLE”. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings: 9,600 baud, 8 data bits, no parity, 1 stop bit, no flow control.
3. Press **Return**. Initial information is displayed followed by an `SCA>` prompt.
4. Enter Privileged and Configuration modes and set the IP address using the following commands. Replace the IP address in the example with the appropriate one.

```
SCA> enable
SCA# configure
(config[SCA])# ip address 10.1.2.5
(config[SCA])#
```

**Note**

---

When prompted to supply a file name during serial management, you must supply it as a URL in the form of HOST/PATH/FILENAME using the http://, https://, ftp://, or tftp:// prefix.

---

## Telnet

After you have assigned an IP address to the Cisco Secure Content Accelerator using the serial connection or remote configuration manager, you can connect to the appliance via telnet.

1. Initiate a telnet session with the IP address previously assigned to the appliance.
2. An SCA> prompt is displayed.

**Note**

---

When prompted to supply a file name during a telnet management session, you must supply it as a URL in the form of HOST/PATH/FILENAME using the http://, https://, ftp://, or tftp:// prefix.

---

## Running the Remote Configuration Manager

Use the appropriate instructions below to run the CLI configuration manager.

### Linux

Enter **csacfg** at a Linux shell prompt.

### Solaris

Enter **csacfg** at a Unix shell prompt.

## Windows NT and Windows 2000 Software

To start the configuration manager, use the **Start** menu and point to **Programs>Cisco Systems** and click **Cisco Secure Content Acc. Manager**, or double-click the shortcut on the desktop.

## Using the Remote Configuration Manager

Enter **show device list** to display a list of all Cisco Secure Content Accelerators in the same broadcast domain as the configuring computer and those found using the discover port command. Devices are listed in the following format:

Type	Key	Name	Version	MacAddr	IPAddr
------	-----	------	---------	---------	--------

Cisco Secure Content Accelerator devices are listed with the “CSS-SCA” device type. Note the MAC address of the device you wish to configure. It is used with the “CS-” prefix to identify a specific device when giving commands in the format *CS-macaddress*, where *macaddress* is the MAC address of the device.



### Note

Identify an unnamed device as a specific appliance, match the last six digits of the serial number with the MAC address shown.

## Specifying Devices

If only one device is listed, you can configure it by simply entering commands as listed. If multiple devices are listed, you must specify the device your commands should address. In these instances you must use the **on** prefix.

For example, entering **show device list** returns the following list of unattached devices:

CSS-SCA	Ru	sslDev1	...
CSS-SCA	Ru	sslDev2	...
CSS-SCA	Ru	sslDev3	...
CSS-SCA2	Ru	sslDev4	...

Secure Content Accelerator version 2 devices are indicated by the type CSS-SCA2.

To attach the configuration manager to the device *sslDev3*, enter this command:

```
on sslDev3 attach
```

The auto completer function can assist data entry. See “Editing and Completion Features” in Appendix C for details for using editing and auto completer features.

## Working with Device Groups

The remote configuration manager allows you to create groups of devices for single management sessions. Most Top Level commands can target a group just as they would a single device. Using the device list above, the commands below create a device group named *myGroup*, add three devices, and display the group contents.

```
csacfg> group myGroup create
(group[myGroup])> device sslDev1
(group[myGroup])> device sslDev2
(group[myGroup])> device sslDev4
(group[myGroup])> info
group name: myGroup
number of devices: 3
device: sslDev1
device: sslDev2
device: sslDev4
(group[myGroup])>
```

To remove a device from the group, use the **no** form of the command:

```
(group[myGroup])> no device sslDev2
```

Enter **end** to leave Group configuration mode. To send commands to every device in the group, use the **on** prefix.

```
on myGroup attach
```

You can simplify command entry for this group further by setting the **on** command to address the group *myGroup* by default.

```
set on-prefix myGroup
```

After entering this command, you do not need to use the **on** prefix when addressing the default target. For example, the **on myGroup attach** command becomes **attach**. You can still address another group instead of the default; simply

specify its name following the **on** prefix. Change the **on** prefix target by re-entering the command, identifying the new group. View the **on** prefix target by entering **show profile**.

**Note**

---

Individual devices can also be set as the **on** prefix default target. Any command without the **on** prefix defaults to the group or device specified by the **set on-prefix** command.

---

For more information about Group Configuration commands, see “Group Configuration Command Set” in Appendix C.

## Remote Configuration Caching

The remote configuration manager caches some management session information. Some changes made during a configuration session may not be displayed. Additionally, configuration changes from multiple concurrent configuration sessions may not be reflected in status and configuration displays. To obtain the most current configuration data, exit the configuration manager, and launch the application again or use the **refresh** command in the Privileged Command set.



# Top Level Command Set

The Top Level command set consists of Non-Privileged and Privileged commands. These commands are used to view and clear statistics and device status, set terminal configuration, enter configuration modes, manage hardware, and exit the configuration manager.

## Non-Privileged Command Set

The Non-Privileged command set consists of the lowest level commands having the least impact on configuration and security of the devices.

### attach

Attaches or detaches the configuration manager from one or more devices.

**attach**

**no attach**

**on <devname|groupname|all> attach**

**on <devname|groupname|all> no attach**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of a user-defined group of devices.
	<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**Availability: *Remote*

Use the simple **attach** form of the command to attach to a single found device. Use the **no** form of the command to detach the configuration manager from a single attached device. If an access-level password has been defined, you must enter it when prompted before the configuration manager will attach to the device(s). If a shared secret passphrase has been assigned as part of remote management encryption, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Note**


---

If you have forgotten the device's access password, see "Factory Default Reset Password".

---



---

**Related Commands****attach ip** (Non-Privileged Command Set)**enable** (Non-Privileged Command Set)**remote-management enable** (Configuration Command Set)**remote-management port** (Configuration Command Set)**attach ip**

Attaches or detaches the configuration manager from one or more devices using an alternate remote management port.

**attach ip** <ipaddr> [**port** <portid>]

**no attach ip** <ipaddr>

---

**Syntax Description**

<i>ipaddr</i>	The IP address of the Secure Content Accelerator.
<i>portid</i>	The TCP service port number.

---

---

**Usage Guidelines**

Availability: *Remote*

Use the **port** option to specify a TCP/UDP service port to use for attaching to the device. The **remote-management port** command must have been used on the device to change the management port from the default. If a shared secret passphrase has been assigned as part of remote management encryption, you are prompted for it. Use the **no** form of the command to detach the configuration manager from the specified device. If an access-level password has been defined, you must enter it when prompted before the configuration manager can attach to the device.

**Note**

---

If you have forgotten the device's access password, see "Factory Default Reset Password".

---

---

**Related Commands**

**attach** (Non-Privileged Command Set)

**enable** (Non-Privileged Command Set)

**remote-management enable** (Configuration Command Set)

**remote-management port** (Configuration Command Set)

---

**clear screen**

Clears the display, leaving only one prompt line.

**clear screen**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**cls**

Clears the display, leaving only one prompt line.

**cls**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## discover

Checks the network for new remote devices on the default or, optionally, on the specified TCP service port when using an alternate remote management port.

**discover [port <portid>]**

<b>Syntax Description</b>	<i>portid</i>	The port number.
---------------------------	---------------	------------------

<b>Usage Guidelines</b>	Availability: <i>Remote</i>
	Use the <b>port</b> option to specify a TCP service port to search for devices when using an alternate remote management port.

<b>Related Commands</b>	<b>remote-management port</b> (Configuration Command Set)
-------------------------	---

## enable

Enters or leaves Privileged Mode for one or more attached device.

**enable**

**no enable**

**on <devname|groupname|all> enable**

**on <devname|groupname|all> no enable**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of a user-defined group of devices.
	<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If an enable-level password has been defined, you must enter it when prompted. When using remote management, enters Privileged mode for a single, attached device. Using the **no** form of this command leaves Privileged mode. When using remote configuration, use the **on** form of the command to specify the target(s) of the command when more than one device is appropriate.

**Note**

---

If you have forgotten the device's enable password, see "Factory Default Reset Password".

---

---

**Related Commands**

**attach** (Non-Privileged Command Set)

**attach ip** (Non-Privileged Command Set)

See the section "Privileged Command Set".

**exit**

Quits the configuration manager.

**exit**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When executed from the remote configuration manager, closes the configuration manager. When executed from a serial connection, the connection is not closed. If an access password has been configured, you are prompted for it. When executed from telnet, the telnet connection is closed.

---

**Related Commands**

**quit** (Non-Privileged Command Set)

## group

Creates or configures the specified user-defined device group.

```
group <groupname> [create]
no group <groupname>
```

Syntax Description	<i>groupname</i>	The name of a user-defined group of devices.
	<b>create</b>	Creates a new device group named <i>groupname</i> and enters Group Configuration Mode for that device group.

### Usage Guidelines

Availability: *Remote*

Use the **create** flag to create the specified group and enter Group Configuration mode for it. Use the **no** form of the command to remove the specified group.

### Related Commands

See also “Group Configuration Command Set”.

## help

Displays help information for the specified command.

```
help [command]
```

Syntax Description	<i>command</i>	The name of the command.
--------------------	----------------	--------------------------

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If no command is specified, help information is displayed for all Non-Privileged commands. When using remote configuration, help information is displayed for all Top Level commands.

## monitor

Displays the results of the specified command at one second intervals.

**monitor** <command>

---

### Syntax Description

<i>command</i>	The name of the command.
----------------	--------------------------

---



---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The interval between refreshes is set using the **set monitor-interval** command.

---

### Related Commands

**set monitor-interval** (Non-Privileged Command Set)

**show profile** (Non-Privileged Command Set)

## paws

Pauses the configuration manager until a key is pressed.

**paws**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## ping

Sends ICMP packets to the specified IP address.

**ping** <ipaddr|name>

---

### Syntax Description

<i>ipaddr</i>	The specified destination IP address.
<i>name</i>	The name of the host to ping (serial or telnet only).

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The host name can be used remotely if a domain name has been assigned for the device. When issued from a serial or telnet connection, the command returns information based upon the hardware of the Secure Content Accelerator. When issued from a remote management connection, the command returns information based upon the configuring computer.

---

**Related Commands**

**ip name-server** (Configuration Command Set)

**quit**

Quits the configuration manager.

**quit**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When executed from the remote configuration manager, closes the configuration manager. When executed from a serial connection, the connection is not closed. If an access password has been configured, you are prompted for it. When executed from telnet, the telnet connection is closed.

---

**Related Commands**

**exit** (Non-Privileged Command Set)

**set monitor-interval**

Sets the number of seconds between monitor-prefixed command refreshes.

**set monitor-interval** <value>  
**no set monitor-interval**

---

**Syntax Description**

---

<i>value</i>	The number of seconds between refreshes
--------------	---

---



---

**Usage Guidelines**Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*Use the **no** form of the command to return the monitor interval to default value.

---

**Related Commands****monitor** (Non-Privileged Command Set)**show profile** (Non-Privileged Command Set)**set on-prefix**Sets the entity to address as default when using the **on** prefix.

```

set on-prefix <devname|groupname|all>
no set on-prefix

```

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator to target
<i>groupname</i>	The name of the user-defined device group to target

---

**Usage Guidelines**Availability: *Remote*Use the **no** form of the command to clear the default entity.

---

**Related Commands****group** (Non-Privileged Command Set)**show profile** (Non-Privileged Command Set)**show arp**

Displays the ARP cache on the specified device.

```

show arp
on <devname|groupname|all> show arp

```

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show copyrights**

Displays copyright information for software and hardware products.

**show copyrights****Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**show version** (Non-Privileged Command Set)

**show cpu**

Displays CPU utilization information for one or more devices.

**show cpu [continuous] [interval <value>]**

**on <devname|groupname|all> show cpu [continuous] [interval <value>]**

<b>Syntax Description</b>	<b>continuous</b>	Displays statistics continuously updated at one-second intervals.
	<b>interval</b>	Specifies an interval for display updates.
	<i>value</i>	The interval in seconds.
	<i>devname</i>	The name of the Secure Content Accelerator.

<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **continuous** option to have statistics displayed continuously, updated at one-second intervals. Use the **interval** option to specify an interval for display updates. Press any key to stop displaying statistics. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

## show date

Displays current date and time settings on the device.

**show date**

### Usage Guidelines

Availability: *Serial, Telnet; FIPS Mode (serial only)*

### Related Commands

**rdate-server** (Configuration Command Set)

## show device

Displays information about the specified device(s).

**show device**

**on <devname|groupname|all> show device**

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show device list**

Displays summary information for all Secure Content Accelerators in the same broadcast domain as the configuring computer or found by the configuration manager after launching the configuration manager and using the **discover** command.

**show device list**

---

**Usage Guidelines**Availability: *Remote*

Devices are listed in the following format:

Type	Key	Name	Version	MacAddr	IPAddr
------	-----	------	---------	---------	--------

Note the MAC address of the device you wish to configure. It is used with the “CS-” prefix to identify a specific device when giving commands.

---

**Related Commands****discover** (Non-Privileged Command Set)**show dns**

Displays DNS configuration information for one or more devices.

**show dns****on** *<devname|groupname|all>* **show dns**

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**ip domain-name** (Configuration Command Set)

**show ip domain-name** (Non-Privileged Command Set)

**show ip name-server** (Non-Privileged Command Set)

## show flows

Displays IP connection information for one or more devices.

**show flow**

**on** <devname|groupname|all> **show flow**

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

## show group

Displays group summary information for the specified group.

**show group** [*groupname*]

---

**Syntax Description**

<i>groupname</i>	The name of the user-defined device group.
------------------	--

---

**Usage Guidelines**Availability: *Remote*

If a group is not specified, information is displayed for all groups.

---

**Related Commands****group** (Non-Privileged Command Set)

See the section “Group Configuration Command Set”.

**show history**

Displays the last commands executed.

**show history**

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands****show terminal** (Top Level Command Set)**terminal history** (Top Level Command Set)**show interface**

Displays information for the specified Ethernet interface on one or more devices.

**show interface [network | server]****on <devname|groupname|all> show interface [network | server]**

---

**Syntax Description**

<b>network</b>	Displays information for the “Network” interface.
<b>server</b>	Displays information for the “Server” interface.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The information includes connection, duplex, speed, and autonegotiation settings. If a single interface is not specified, information is displayed for all interfaces on the device(s). When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show interface errors** (Non-Privileged Command Set)  
**show interface statistics** (Non-Privileged Command Set)  
**interface** (Configuration Command Set)

See the section “Interface Configuration Command Set”.

**show interface errors**

Displays error information for the specified Ethernet interface on one or more devices.

**show interface errors** [**network** | **server**] [**continuous**] [**interval** <value>]

**on** <devname|groupname|all> **show interface errors** [**network** | **server**]  
 [**continuous**] [**interval** <value>]

**Syntax Description**

<b>network</b>	Displays information for the “Network” interface.
<b>server</b>	Displays information for the “Server” interface.
<b>continuous</b>	Displays errors continuously.
<b>interval</b>	Specifies an interval for display updates.
<i>value</i>	The interval in seconds.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If a single interface is not specified, errors are displayed for both interfaces. If continuous is specified, error statistics are updated every second. Use the **interval** option to specify an interval for display updates. Press any key to stop displaying errors. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**show interface** (Non-Privileged Command Set)  
**show interface statistics** (Non-Privileged Command Set)  
**interface** (Configuration Command Set)

See the section “Interface Configuration Command Set”.

## show interface statistics

Displays interface statistics for one or more devices.

```
show interface statistics [network | server] [continuous] [interval
  <value>]
```

```
on <devname|groupname|all> show interface statistics [network | server]
  [continuous] [interval <value>]
```

---

**Syntax Description**

<b>network</b>	Displays information for the “Network” interface.
<b>server</b>	Displays information for the “Server” interface.
<b>continuous</b>	Displays statistics continuously.
<b>interval</b>	Specifies an interval for display updates.
<i>value</i>	The interval in seconds.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.



**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If a single interface is not specified, statistics are displayed for both interfaces. If **continuous** is specified, statistics are updated every second. Use the **interval** option to specify an interval for display updates. Press any key to stop displaying statistics. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show interface** (Non-Privileged Command Set)  
**show interface errors** (Non-Privileged Command Set)  
**interface** (Configuration Command Set)

See the section “Interface Configuration Command Set”.

**show ip domain-name**

Displays DNS configuration information for one or more devices.

**show ip domain-name**

**on** <devname|groupname|all> **show ip domain-name**

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**ip domain-name** (Configuration Command Set)  
**show dns** (Non-Privileged Command Set)  
**show ip name-server** (Non-Privileged Command Set)

## show ip name-server

Displays DNS configuration information for one or more devices.

**show ip name-server**

**on** <devname|groupname|all> **show ip name-server**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command when more than one device is appropriate.

### Related Commands

**ip domain-name** (Configuration Command Set)

**show dns** (Non-Privileged Command Set)

**show ip domain-name** (Non-Privileged Command Set)

## show ip routes

Displays the routing table stored in one or more devices.

**show ip routes**

**on** <devname|groupname|all> **show ip routes**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show route** (Non-Privileged Command Set)

**show ip statistics**

Displays diagnostic IP, ICMP, TCP, and UDP statistics for one or more devices.

**show ip statistics**

**on** <devname|groupname|all> **show ip statistics**

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show keepalive-monitor**

Displays a list of keepalive-monitor IP addresses for one or more devices.

**show keepalive-monitor**

**on** <devname|groupname|all> **show keepalive-monitor**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

SSL errors from IP addresses specified with the **keepalive-monitor** command are ignored. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**keepalive-monitor** (Configuration Command Set)

**show memory**

Displays memory usage on one or more devices.

**show memory [zones]**

**on <devname|groupname|all> show memory [zones]**

<b>Syntax Description</b>	<b>zones</b>	Specifies memory information for each zone is to be displayed.
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **zones** flag is used to display information for each memory zone. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

## show messages

Displays the diagnostic message buffer for one or more devices.

**show messages**

**on** <devname|groupname|all> **show messages**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**clear messages** (Non-Privileged Command Set)

**write messages** (Privileged Command Set)

## show netstat

Displays the current state of the IP connection for one or more devices.

**show netstat**

**on** <devname|groupname|all> **show netstat**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show processes**

Displays information, by thread, about processes running on one or more devices.

**show processes**

**on** <devname|groupname|all> **show processes**

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show profile**

Displays the **monitor-interval** and **on-prefix** settings of the if they have been changed from the default settings.

**show profile [all]**

---

**Syntax Description**

<b>all</b>	Displays current settings for both <b>monitor-interval</b> and <b>on-prefix</b> .
------------	---

**Usage Guidelines**

Availability: *Remote*

Use the **all** keyword to display the current configuration of both the monitor-interval and on-prefix.

**Related Commands**

**monitor** (Non-Privileged Command Set)  
**set monitor-interval** (Non-Privileged Command Set)  
**set on-prefix** (Non-Privileged Command Set)

**show rdate-server**

Displays the IP address of the RDATE protocol server configuration for one or more devices.

**show rdate-server**

**on** <devname|groupname|all> **show rdate-server**

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**show remote-management**

Displays remote management information for one or more devices.

**show remote-management**

**on** <devname|groupname|all> **show remote-management**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**remote-management access-list** (Configuration Command Set)  
**remote-management enable** (Configuration Command Set)  
**remote-management encryption** (Configuration Command Set)  
**remote-management port** (Configuration Command Set)  
**remote-management shared-secret** (Configuration Command Set)  
**show telnet** (Non-Privileged Command Set)  
**show web-management** (Non-Privileged Command Set)

**show rip**

Displays the RIP status of one or more devices.

**show rip**

**on** <*devname*|*groupname*|**all**> **show rip**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.



**Related Commands**    **rip** (Configuration Command Set)

## show route

Displays the routing table stored in one or more devices.

**show route**

**on** <devname|groupname|all> **show route**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**    **show ip routes** (Top Level Command Set)

## show sessions

Displays current remote configuration manager, serial, and telnet management connections to the device.

**show sessions**

### Usage Guidelines

Availability: *Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**    **clear line** (Privileged Command Set)

## show sntp-server

Displays SNTP-server information for one or more devices. The SNTP server is used for date and time information.

**show sntp-server**

**on** <devname|groupname|all> **show sntp-server**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**sntp-server** (Configuration Command Set)

## show ssl

Displays SSL summary data for one or more devices.

**show ssl**

**on** <devname|groupname|all> **show ssl**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the section “SSL Configuration Command Set”.

**show ssl cert**

Displays summary data for the specified certificate entity loaded on one or more devices.

```
show ssl cert [certname]
```

```
on <devname|groupname|all> show ssl cert [certname]
```

**Syntax Description**

<i>certname</i>	The name of the certificate.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a certificate name, all certificate entity information is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl errors all** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**show ssl statistics all** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the sections “SSL Configuration Command Set”, “Certificate Configuration Command Set”, and “Certificate Group Configuration Command Set”.

**show ssl certgroup**

Displays summary data for the specified certificate group loaded on one or more devices.

**show ssl certgroup** [*certgroupname*]

**on** <*devname*|*groupname*|**all**> **show ssl certgroup** [*certgroupname*]

**Syntax Description**

<i>certgroupname</i>	The name of the certificate group.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a certificate group, all certificate group information is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the sections “SSL Configuration Command Set”, “Certificate Configuration Command Set”, and “Certificate Group Configuration Command Set”.

**show ssl errors**

Displays SSL errors reported on one or more devices.

**show ssl errors** [**continuous**] [**interval** <value>]

**on** <devname|groupname|all> **show ssl errors** [**continuous**] [**interval** <value>]

**Syntax Description**

<b>continuous</b>	Displays errors continuously.
<b>interval</b>	Specifies an interval for display updates.
<i>value</i>	The interval in seconds.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

(This command must be given on one line.) Displays SSL errors reported on a single device or module. Use the **continuous** keyword to update the statistics every second. Use the **interval** keyword to specify an interval for display updates, where value is the interval in seconds. Press any key to stop displaying errors. When using remote configuration, use the **on** form of the command to specify the target(s) of the command, where *devname* is the name of a single device or module, *groupname* is the name of a user-defined device group, and **all** represents all appropriate devices and modules. Table C-3 displays output descriptions.

**Table C-3 Output Description for show ssl errors**

Error	Description
SSL Negotiation Errors	The number of SSL negotiation failures
Total SSL Connections Rejected	The number of SSL connections rejected when the pre-defined limit of connections has been exceeded
SSL Accept Errors	Generated when SSL connection acceptance fails; eight states are recognized: 0 SSL_ERROR_NONE 1 SSL_ERROR_SSL 2 SSL_ERROR_WANT_READ 3 SSL_ERROR_WANT_WRITE 4 SSL_ERROR_WANT_X509_LOOKUP 5 SSL_ERROR_SYSCALL 6 SSL_ERROR_ZERO_RETURN 7 SSL_ERROR_WANT_CONNECT
SSL System Write Errors to client	Generated when an error occurs when writing to a client
SSL Write Broken Connection Error to client	Generated when writing to the client after the client has reset the connection
SSL System Read Errors from client	Generated when an error occurs when reading from a client
SSL Read Broken Connection Error from client	Generated when reading from a client after the client has reset the connection

**Table C-3** *Output Description for show ssl errors (continued)*

Error	Description
System Write Errors to remote server	Generated when an error occurs when writing to a remote server
Broken Connection Write Errors to remote server	Generated when writing to a remote server after the remote server as reset the connection
System Read Errors from remote server	Generated when reading from a remote server
Broken Connection Read Errors from remote server	Generated when reading from a remote server after the remote server as reset the connection

**Table C-3** Output Description for show ssl errors (continued)

Error	Description
System Call Error Histogram for Client SSL Connections	<p>Generated with the client connection is closed; histogram errors include:</p> <ul style="list-style-type: none"> <li>"No buffers available"</li> <li>"Operation timed out"</li> <li>"Socket is connected"</li> <li>"Operation not supported"</li> <li>"Connection aborted"</li> <li>"Operation would block"</li> <li>"Connection refused"</li> <li>"Connection reset by peer"</li> <li>"Socket not connected"</li> <li>"Message size error"</li> <li>"Pipe error"</li> <li>"EDESTADDRREQ"</li> <li>"EDESTADDRREQ"</li> <li>"Socket shutdown"</li> <li>"Unsupported protocol option"</li> <li>"Out of band data"</li> <li>"Address is not available"</li> <li>"Address already in use"</li> <li>"Address family is not supported"</li> <li>"Operation already in progress"</li> <li>"lower error"</li> <li>"I/O error"</li> <li>"Destination host is down"</li> <li>"Unsupported protocol"</li> <li>"Destination network is down"</li> <li>"Destination host unreachable"</li> <li>"Destination network unreachable"</li> <li>"Protocol Family not supported"</li> <li>"Prototype error"</li> </ul>



**Table C-3** Output Description for show ssl errors (continued)

Error	Description
System Call Error Histogram for Server Connections	<p>Generated with the server connection is closed; histogram errors include:</p> <ul style="list-style-type: none"> <li>"No buffers available"</li> <li>"Operation timed out"</li> <li>"Socket is connected"</li> <li>"Operation not supported"</li> <li>"Connection aborted"</li> <li>"Operation would block"</li> <li>"Connection refused"</li> <li>"Connection reset by peer"</li> <li>"Socket not connected"</li> <li>"Message size error"</li> <li>"Pipe error"</li> <li>"EDESTADDRREQ"</li> <li>"EDESTADDRREQ"</li> <li>"Socket shutdown"</li> <li>"Unsupported protocol option"</li> <li>"Out of band data"</li> <li>"Address is not available"</li> <li>"Address already in use"</li> <li>"Address family is not supported"</li> <li>"Operation already in progress"</li> <li>"lower error"</li> <li>"I/O error"</li> <li>"Destination host is down"</li> <li>"Unsupported protocol"</li> <li>"Destination network is down"</li> <li>"Destination host unreachable"</li> <li>"Destination network unreachable"</li> <li>"Protocol Family not supported"</li> <li>"Prototype error"</li> </ul>

The errors displayed when using the **continuous** or **interval** keywords are listed in Table C-4 below.

**Table C-4 Abbreviations Used for show ssl errors continuous**

Abbreviation	Description
ACPT	SSL Accept Errors
SSLW	SSL System Write Errors to Client
SSLWBC	SSL System Write Broken Connection Errors to Client
SSLR	SSL System Read Errors from Client
SSLRBC	SSL System Read Broken Connection Errors from Client
SVRW	System Write Errors to Remote Server
SVRWBC	Broken Connection Write Errors to Remote Server
SVRR	System Read Errors from Remote Server
SVRRBC	Broken Connection Read Errors from Remote Server

## Related Commands

**keepalive-monitor** (Configuration Command Set)  
**show keepalive-monitor** (Non-Privileged Command Set)  
**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the section “SSL Configuration Command Set”.

## show ssl key

Displays summary data for the specified private key loaded on one or more devices.

```
show ssl key [keyname]
```

```
on <devname|groupname|all> show ssl key [keyname]
```

<b>Syntax Description</b>	<i>keyname</i>	The name of the public/private key pair.
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a key name, all key information is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the sections “SSL Configuration Command Set” and “Key Configuration Command Set”.

**show ssl secpolicy**

Displays summary data for the specified security policy on one or more devices.

**show ssl secpolicy** [*polname*]

**on** <*devname*|*groupname*|**all**> **show ssl secpolicy** [*polname*]

Syntax Description		
	<i>polname</i>	The name of the security policy.
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a security policy name, all security policy information is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the sections “SSL Configuration Command Set” and “Security Policy Configuration Command Set”.

## show ssl server

Displays information for the specified configured logical secure server of type server, reverse-proxy server, or backend server on one or more devices.

```
show ssl server [servname]  

on <devname|groupname|all> show ssl server [servname]
```

**Syntax Description**

<i>servername</i>	The name of the server.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a secure server name, all secure server information is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the sections “SSL Configuration Command Set” and “Server Configuration Command Set”.

**show ssl session-stats**

Displays SSL session statistics summed over all secure logical servers on one or more devices.

**show ssl session-stats [continuous] [interval <value>]**

**on <devname|groupname|all> show ssl session-stats [continuous] [interval <value>]**

Syntax Description		
	<b>continuous</b>	Displays statistics continuously.
	<b>interval</b>	Specifies an interval for display updates.
	<i>value</i>	The interval in seconds.
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **continuous** keyword to update the statistics every second. Use the **interval** keyword to specify an interval for display updates. Press any key to stop displaying information. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the section “SSL Configuration Command Set”.

## show ssl statistics

Displays SSL statistics summed over all secure logical servers on one or more devices.

```
show ssl statistics [continuous] [interval <value>]
```

```
on <devname|groupname|all> show ssl statistics [continuous] [interval <value>]
```

Syntax Description		
	<b>continuous</b>	Displays statistics continuously.
	<b>interval</b>	Specifies an interval for display updates.
	<i>value</i>	The interval in seconds.
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **continuous** keyword to update the statistics every second. Use the **interval** keyword to specify an interval for display updates. Press any key to stop displaying information. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate. Table C-5 displays output descriptions.

**Table C-5** Output Description for *show ssl statistics*

Statistic	Description
Active Client Connections	The number of client connections currently active
Active Server Connections	The number of server connections currently active
Active Sockets	The number of currently active sockets
SSL Negotiation Errors	The number of SSL negotiation failures
Connection Errors to remote Server	The number of errors encountered when connecting to remote (backend) servers
Total Connection Block Errors	The number of errors generated during connections
Total SSL Connections Refused	The number of SSL connections refused

**Table C-5** *Output Description for show ssl statistics (continued)*

Statistic	Description
Total SSL Connections Rejected	The number of SSL connections rejected when the pre-defined limit of connections has been exceeded
Total Connections Accepted	The number of client connections accepted
Total RSA Operations in Hardware	The number of RSA operations performed by the Secure Content Accelerator
Total SSL Negotiations Succeeded	The number of successful SSL negotiations

The statistics displayed when using the **continuous** or **interval** keywords are listed in Table C-6 below.

**Table C-6** *Abbreviations Used for show ssl statistics continuous*

Abbreviation	Description
AC	Active Client Connections, Active Server Connections
AS	Active Sockets
SNE	SSL Negotiation Errors
TSE	Total Socket Errors
CES	Connection Errors to Remote Server
TCBE	Total Connection Block Errors
TSCR	Total SSL Connections Refused, Total SSL Connections Rejected
TCA	Total Connections Accepted
TROH	Total RSA Operations in Hardware
TSNS	Total SSL Negotiations Succeeded






---

**Note** Values for Active Server Connections and Total SSL Connections Refused are not shown when using the **continuous** keyword.

---



---

### Related Commands

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl session-stats** (Non-Privileged Command Set)  
**ssl** (Configuration Command Set)

See the section “SSL Configuration Command Set”.

## show syslog

Displays the list of hosts to which diagnostic messages from one or more devices are sent.

**show syslog**

**on** <devname|groupname|all> **show syslog**

---

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**    `syslog` (Configuration Command Set)

## show system-resources

Displays system memory and CPU usage for one or more devices.

**show system-resources** [**continuous**] [**interval** <value>]

**on** <devname|groupname|all> **show system-resources** [**continuous**]  
[**interval** <value>]

### Syntax Description

<b>continuous</b>	Displays statistics continuously.
<b>interval</b>	Specifies an interval for display updates.
<i>value</i>	The interval in seconds.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **continuous** option to update the information every second. Use the **interval** option to specify an interval for display updates. Press any key to stop displaying information. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

## show telnet

Displays telnet management information for one or more devices.

**show telnet**

**on** <devname|groupname|all> **show telnet**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**telnet access-list** (Configuration Command Set)  
**telnet enable** (Configuration Command Set)  
**telnet port** (Configuration Command Set)  
**show remote-management** (Non-Privileged Command Set)  
**show web-management** (Non-Privileged Command Set)

**show terminal**

Displays terminal setting information.

**show terminal**

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**show history** (Non-Privileged Command Set)  
**terminal baud** (Non-Privileged Command Set)  
**terminal history** (Non-Privileged Command Set)  
**terminal length** (Non-Privileged Command Set)  
**terminal pager** (Non-Privileged Command Set)  
**terminal reset** (Non-Privileged Command Set)  
**terminal width** (Non-Privileged Command Set)

## show version

Displays configuration manager version information.

**show version**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## show web-management

Displays Web-based GUI management information for one or more devices.

**show web-management**

**on** <devname|groupname|all> **show web-management**

---

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

### Related Commands

**web-mgmt access-list** (Configuration Command Set)

**web-mgmt enable** (Configuration Command Set)

**web-mgmt port** (Configuration Command Set)

**show remote-management** (Non-Privileged Command Set)

**show telnet** (Non-Privileged Command Set)

## terminal baud

Sets the baud for communicating with the Secure Content Accelerator.

**terminal baud <1200|2400|4800|9600|19200|38400|115200>**

Syntax Description		
	<b>1200</b>	Sets the baud to 1200.
	<b>2400</b>	Sets the baud to 2400.
	<b>4800</b>	Sets the baud to 4800.
	<b>9600</b>	Sets the baud to 9600.
	<b>19200</b>	Sets the baud to 19,200.
	<b>38400</b>	Sets the baud to 38,400.
	<b>115200</b>	Sets the baud to 115,200.

### Usage Guidelines

Availability: *Serial; FIPS Mode (serial only)*

### Related Commands

**show terminal** (Non-Privileged Command Set)  
**terminal history** (Non-Privileged Command Set)  
**terminal length** (Non-Privileged Command Set)  
**terminal pager** (Non-Privileged Command Set)  
**terminal reset** (Non-Privileged Command Set)  
**terminal width** (Non-Privileged Command Set)

## terminal history

Sets the number of commands saved in the history buffer. Use the **no** form of the command to disable the history list.

**terminal history <length>**  
**no terminal history**

<b>Syntax Description</b>	<i>length</i>	The number of commands to store in the history buffer.
---------------------------	---------------	--

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i> The default is 25.	
-------------------------	--	--

<b>Related Commands</b>	<b>show history</b> (Non-Privileged Command Set) <b>show terminal</b> (Non-Privileged Command Set) <b>terminal baud</b> (Non-Privileged Command Set) <b>terminal length</b> (Non-Privileged Command Set) <b>terminal pager</b> (Non-Privileged Command Set) <b>terminal reset</b> (Non-Privileged Command Set) <b>terminal width</b> (Non-Privileged Command Set)	
-------------------------	---	--

## terminal length

Sets the number of lines in a terminal window.

### **terminal length**

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>	
-------------------------	--	--

<b>Related Commands</b>	<b>show terminal</b> (Non-Privileged Command Set) <b>terminal baud</b> (Non-Privileged Command Set) <b>terminal history</b> (Non-Privileged Command Set) <b>terminal pager</b> (Non-Privileged Command Set) <b>terminal reset</b> (Non-Privileged Command Set) <b>terminal width</b> (Non-Privileged Command Set)	
-------------------------	--	--

## terminal pager

Enables the terminal pager. Using the **no** form of the command disables the pager.

**terminal pager**  
**no terminal pager**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

### Related Commands

**show terminal** (Non-Privileged Command Set)  
**terminal baud** (Non-Privileged Command Set)  
**terminal history** (Non-Privileged Command Set)  
**terminal length** (Non-Privileged Command Set)  
**terminal reset** (Non-Privileged Command Set)  
**terminal width** (Non-Privileged Command Set)

## terminal reset

Resets the internal state of the terminal.

**terminal reset**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

### Related Commands

**show terminal** (Non-Privileged Command Set)  
**terminal baud** (Non-Privileged Command Set)  
**terminal history** (Non-Privileged Command Set)  
**terminal length** (Non-Privileged Command Set)  
**terminal pager** (Non-Privileged Command Set)  
**terminal width** (Non-Privileged Command Set)

## terminal width

Sets the width of the terminal window.

**terminal width** <width>

<b>Syntax Description</b>	<i>width</i>	The desired width of the terminal window.
---------------------------	--------------	---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>	
-------------------------	--	--

<b>Related Commands</b>	<b>show terminal</b> (Non-Privileged Command Set) <b>terminal baud</b> (Non-Privileged Command Set) <b>terminal history</b> (Non-Privileged Command Set) <b>terminal length</b> (Non-Privileged Command Set) <b>terminal pager</b> (Non-Privileged Command Set) <b>terminal reset</b> (Non-Privileged Command Set)
-------------------------	---

## traceroute

Displays the router hops to the specified destination.

**traceroute** <ipaddr|name>

<b>Syntax Description</b>	<i>ipaddr</i>	The destination IP address.
	<i>name</i>	The name of the destination host (serial or telnet only).

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>  When issued from a serial or telnet connection, the command returns information based upon the device's hardware. When issued from the remote configuration manager, the command returns information based upon the configuring computer.
-------------------------	---



## Privileged Command Set

Use Privileged mode commands to view and edit device-specific configuration information. Enter Privileged mode for a device by using the **enable** command in Non-Privileged mode. All Non-Privileged commands are also available.

### clear interface statistics

Resets all interface statistics for one or more devices.

**clear interface statistics**

**on** <devname|groupname|all> **clear interface statistics**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**show interface** (Non-Privileged Command Set)  
**show interface errors** (Non-Privileged Command Set)  
**show interface statistics** (Non-Privileged Command Set)  
**interface** (Configuration Command Set)

See “Interface Configuration Command Set”.

## clear ip routes

Clears the IP routing table on one or more devices.

**clear ip routes**

**on** <devname|groupname|all> **clear ip routes**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**show ip routes** (Non-Privileged Command Set)

**show routes** (Non-Privileged Command Set)

**ip route** (**Configuration** Command Set)

## clear ip statistics

Resets all IP statistics on one or more devices.

**clear ip statistics**

**on** <devname|groupname|all> **clear ip statistics**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**show ip statistics** (Non-Privileged Command Set)

## clear line

Closes a specified management session.

**clear line** <sessionId>

---

**Syntax Description**

---

<i>sessionId</i>	The session identifier
------------------	------------------------

---

---

**Usage Guidelines**

Availability: *Serial; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate. Use the show sessions command to display the open management sessions.

---

**Related Commands**

**show sessions** (Non-Privileged Command Set)

## clear messages

Empties the diagnostic message buffer on one or more devices.

**clear messages**

**on** <devname|groupname|all> **clear messages**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands** **show messages** (Non-Privileged Command Set)  
**write messages** (Privileged Command Set)

## clear ssl session-stats

Resets all SSL session statistics for one or more devices.

**clear ssl session-stats**

**on** <*devname|groupname|all*> **clear ssl session-stats**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands** **show ssl errors** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)

## clear ssl statistics

Resets all SSL statistics for one or more devices.

**clear ssl statistics**

**on** <devname|groupname|all> **clear ssl statistics**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**show ssl errors** (Non-Privileged Command Set)

**show ssl statistics** (Non-Privileged Command Set)

## configure

Enters Configuration mode for a device in Privileged mode.

**configure**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### Related Commands

See the section “Configuration Command Set”.

## copy running-configuration

Writes the running-configuration of a device to a file.

**copy running-configuration** [*filename|url*]

**on** <*devname*> **copy running-configuration** [*filename*]

### Syntax Description

<i>filename</i>	The name of the file, including its path.
<i>url</i>	The URL of the file (serial and telnet only).
<i>devname</i>	The name of the Secure Content Accelerator.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a file name or URL, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target of the command if more than one device is appropriate.

### Related Commands

**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration** (Privileged Command Set)  
**copy startup-configuration running configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**copy to startup-configuration** (Privileged Command Set)

## copy running-configuration startup-configuration

Writes the running-configuration of a device to its startup-configuration.

**copy running-configuration startup-configuration**

### Usage Guidelines

Availability: *Serial, Telnet; FIPS Mode (serial only)*

---

<b>Related Commands</b>	<b>copy running-configuration</b> (Privileged Command Set) <b>copy startup-configuration</b> (Privileged Command Set) <b>copy startup-configuration running configuration</b> (Privileged Command Set) <b>copy to running-configuration</b> (Privileged Command Set) <b>copy to startup-configuration</b> (Privileged Command Set)
-------------------------	--

## copy startup-configuration

Writes the startup-configuration of a device to a file.

**copy startup-configuration** *<url>*

---

<b>Syntax Description</b>	<i>url</i> The URL of the file.
---------------------------	---------------------------------

---

---

<b>Usage Guidelines</b>	Availability: <i>Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--

---

<b>Related Commands</b>	<b>copy running-configuration</b> (Privileged Command Set) <b>copy running-configuration startup-configuration</b> (Privileged Command Set) <b>copy startup-configuration running configuration</b> (Privileged Command Set) <b>copy to running-configuration</b> (Privileged Command Set) <b>copy to startup-configuration</b> (Privileged Command Set)
-------------------------	--

## copy startup-configuration running-configuration

Writes the startup-configuration of a device to its running-configuration.

**copy startup-configuration running-configuration**

---

<b>Usage Guidelines</b>	Availability: <i>Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--

**Related Commands**

**copy running-configuration** (Privileged Command Set)  
**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**copy to startup-configuration** (Privileged Command Set)

**copy to flash**

Uploads a Cisco Secure Content Accelerator image file to the device flash.

**copy to flash** [*filename*]*[url]*

**on** <*devname*> **copy to flash** [*filename*]

**Syntax Description**

<i>filename</i>	The name of the file, including its path.
<i>url</i>	The URL of the file (serial and telnet only).
<i>devname</i>	The name of the Secure Content Accelerator.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a file name or URL, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.



**Note** When the **copy to flash** command is used in FIPS Mode, the firmware signature is verified.

**Related Commands**

**copy running-configuration** (Privileged Command Set)  
**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**copy to startup-configuration** (Privileged Command Set)



## copy to running-configuration

Uploads a saved configuration file and merges it to the running-configuration of a device.

**copy to running-configuration** [*filename*|*url*]

**on** <*devname*> **copy to running-configuration** [*filename*]

Syntax Description		
	<i>filename</i>	The name of the file, including its path.
	<i>url</i>	The URL of the file (serial and telnet only).
	<i>devname</i>	The name of the Secure Content Accelerator.

### Usage Guidelines

Availability: *Remote*

If you do not specify a file name or URL, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target of the command if more than one device is appropriate.

### Related Commands

**copy running-configuration** (Privileged Command Set)

**copy running-configuration startup-configuration** (Privileged Command Set)

**copy startup-configuration** (Privileged Command Set)

**copy startup-configuration running-configuration** (Privileged Command Set)

**copy to startup-configuration** (Privileged Command Set)

## copy to startup-configuration

Uploads a saved configuration file and merges it to the startup-configuration of a device.

**copy to startup-configuration** [*url*]

Syntax Description		
	<i>url</i>	The URL of the file.

---

**Usage Guidelines**

Availability: *Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a URL, you are prompted for it.

---

**Related Commands**

**copy running-configuration** (Privileged Command Set)

**copy running-configuration startup-configuration** (Privileged Command Set)

**copy startup-configuration** (Privileged Command Set)

**copy startup-configuration running-configuration** (Privileged Command Set)

**copy to running-configuration** (Privileged Command Set)

## disable

Exits Privileged mode for one or more devices.

**disable**

**on** <devname|groupname|all> **disable**

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**enable** (Non-Privileged Command Set)

## erase running-configuration

Erases the running-configuration on one or more devices.

**erase running-configuration**

**on** <devname|groupname|all> **erase running-configuration**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**copy running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**erase startup-configuration** (Privileged Command Set)

## erase startup-configuration

Erases the startup-configuration on one or more devices.

**erase startup-configuration**

**on** <devname|groupname|all> **erase startup-configuration**

Syntax Description		
	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**copy running-configuration** (Privileged Command Set)

**copy to running-configuration** (Privileged Command Set)

**erase running-configuration** (Privileged Command Set)

## fips enable

Starts FIPS-compliant mode for a device in Privileged mode.

**fips enable**  
**no fips enable**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet*

---

**Related Commands**

See the section Chapter 6, FIPS Operation.

## quick-start

Runs the QuickStart wizard for a device.

**quick-start**  
**on <devname> quick-start**

---

**Syntax Description**

---

<i>devname</i>	The name of the Secure Content Accelerator.
----------------	---

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Note**

When using the **quick-start** command in FIPS Mode to create a server, only the FIPS security policy is available. When using the **quick-start** command in FIPS Mode to configure an existing server, only FIPS-compliant servers are available.

---

## refresh

Updates device information in the configuration manager.

**refresh**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## reload

Reboots one or more devices.

**reload**

**on** <devname|groupname|all> **reload**

---

**Syntax Description**

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The device resumes operation using the startup-configuration stored in the flash memory. You are prompted to confirm restarting the device. When using remote configuration, use the **on** form of the command to specify the target(s) of the command.



**Note** You are not prompted to reload devices on a device-by-device basis.



**Note** When reloading the device in FIPS Mode, the firmware signature is verified.

## show access-list

Displays the specified access list for one or more devices.

**show access-list** [*listid*]

**on** <*devname*|*groupname*|**all**> **show access-list** [*listid*]

### Syntax Description

<i>listid</i>	The access list identifier.
<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify an access list id, information for all access lists is displayed. When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

- access-list** (Configuration Command Set)
- remote-management access-list** (Configuration Command Set)
- snmp access-list** (Configuration Command Set)
- telnet access-list** (Configuration Command Set)
- web-mgmt access-list** (Configuration Command Set)

## show diagnostic-report

Displays configuration and diagnostic information for a device.

### **show diagnostic-report**

---

**Usage Guidelines**      Availability: *Serial, Telnet; FIPS Mode (serial only)*

The reports displayed for the device are the following:

- SSL Device Configuration (**show device**)
- Startup Configuration (**show startup-config**)
- Running Configuration (**show running-config**)
- Processes (**show processes**)
- Network Status (**show netstat**)
- Memory Statistics (**show memory**)
- Memory Zones (**show memory zones**)
- SSL Statistics (**show ssl statistics**)
- SSL Session Statistics (**show ssl session-stats**)
- SSL Errors (**show ssl errors**)

Individual reports can be generated using the command displayed between parentheses following each report name.

---

**Related Commands**

- show device** (Non-Privileged Command Set)
- show memory** (Non-Privileged Command Set)
- show memory zones** (Non-Privileged Command Set)
- show netstat** (Non-Privileged Command Set)

**show processes** (Non-Privileged Command Set)  
**show running-config** (Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl session-stats** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)  
**show startup-config** (Privileged Command Set)

## show running-configuration

Displays the running-configuration on one or more devices.

**show running-configuration**

**on** <devname|groupname|all> **show running-configuration**

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**copy running-configuration** (Privileged Command Set)  
**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**erase running-configuration** (Privileged Command Set)  
**show startup-configuration** (Privileged Command Set)  
**write file** (Privileged Command Set)



## show snmp

Displays SNMP configuration information for one or more devices.

**show snmp**

**on** <devname|groupname|all> **show snmp**

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

### Related Commands

**no snmp** (Configuration Command Set)  
**snmp access-list** (Configuration Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp enable** (Configuration Command Set)  
**snmp location** (Configuration Command Set)  
**snmp trap-host** (Configuration Command Set)  
**snmp trap-type enterprise** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)

## show sntp

Displays Sntp configuration information, including the Sntp servers configured and the polling interval.

**show sntp**

**on** <devname|groupname|all> **show sntp**

<b>Syntax Description</b>	<i>devname</i>	The name of the Secure Content Accelerator.
	<i>groupname</i>	The name of the user-defined device group.
	<b>all</b>	A virtual group name targeting all appropriate devices.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

**Related Commands**

**sntp interval** (Configuration Command Set)  
**sntp server** (Configuration Command Set)

**show startup-configuration**

Displays the startup-configuration on a device.

**show startup-configuration**

**Usage Guidelines**

Availability: *Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to flash** (Privileged Command Set)  
**erase start-up-configuration** (Privileged Command Set)  
**show running-configuration** (Privileged Command Set)  
**write flash** (Privileged Command Set)

**write file**

Writes the running-configuration of a device to a file on the file system of the configuring computer.

**write file** [*filename*]

**on** <*devname*> **write file** [*filename*]

### Syntax Description

<i>filename</i>	The name of the file, including the path.
<i>devname</i>	The name of the Secure Content Accelerator.

### Usage Guidelines

Availability: *Remote*

If you do not supply a file name, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target of the command if more than one device is appropriate.

### Related Commands

**copy running-configuration** (Privileged Command Set)  
**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**erase running-configuration** (Privileged Command Set)  
**show running-configuration** (Privileged Command Set)  
**write memory** (Privileged Command Set)

## write flash

Writes the running-configuration to flash memory on one or more devices.

**write flash**

**on** <*devname*|*groupname*|**all**> **write flash**

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.
<b>all</b>	A virtual group name targeting all appropriate devices.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

---

**Related Commands**

**copy running-configuration** (Privileged Command Set)  
**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**erase running-configuration** (Privileged Command Set)  
**show running-configuration** (Privileged Command Set)  
**write memory** (Privileged Command Set)

**write memory**

Writes the running-configuration to flash memory on a device.

**write memory**

---

**Usage Guidelines**

Availability: *Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands**

**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to flash** (Privileged Command Set)  
**erase startup-configuration** (Privileged Command Set)  
**show running-configuration** (Privileged Command Set)  
**write file** (Privileged Command Set)

**write messages**

Writes the diagnostic messages for one or more devices to a file.

**write messages** [*filename*]*[url]*

**on** <*devname*> **write messages** [*filename*]

<b>Syntax Description</b>	<i>filename</i>	The name of the file, including the path.
	<i>url</i>	The URL of the file.
	<i>devname</i>	The name of the Secure Content Accelerator.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not supply a file name, you are prompted for it. When using remote configuration, use the **on** form of the command to specify the target of the command if more than one device is appropriate.

**Related Commands**

**show messages** (Non-Privileged Command Set)

**write network**

Writes the running-configuration to a file on a remote host.

**write network** [*url*]

**Syntax Description**

<i>url</i>	The URL of the file.
------------	----------------------

**Usage Guidelines**

Availability: *Serial, Telnet; FIPS Mode (serial only)*

If you do not supply URL information, you are prompted for it.

**Related Commands**

**copy running-configuration startup-configuration** (Privileged Command Set)  
**copy startup-configuration running-configuration** (Privileged Command Set)  
**copy to running-configuration** (Privileged Command Set)  
**erase running-configuration** (Privileged Command Set)  
**show running-configuration** (Privileged Command Set)

## write terminal

Displays the running-configuration of one or more devices.

### **write terminal**

**on** <*devname*|*groupname*|**all**> **write terminal**

### Syntax Description

<i>devname</i>	The name of the Secure Content Accelerator.
<i>groupname</i>	The name of the user-defined device group.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When using remote configuration, use the **on** form of the command to specify the target(s) of the command if more than one device is appropriate.

# Group Configuration Command Set

Use Group Configuration commands to manage session-specific groups. Enter Group Configuration mode by using the **group** command in Top Level mode.

## device

Adds the specified device to the group list.

```
device <devname>  
no device <devname>
```

---

### Syntax Description

---

<i>devname</i>	The name of the Secure Content Accelerator.
----------------	---

---

---

### Usage Guidelines

Availability: *Remote*

Use the **no** form of the command to remove the specified device from the group list.

## end

Leaves Group Configuration Mode.

```
end
```

---

### Usage Guidelines

Availability: *Remote*

## exit

Leaves Group Configuration Mode.

```
exit
```

---

### Usage Guidelines

Availability: *Remote*

## finished

Exits Group Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote*

## help

Displays information for a specific command.

**help** [*command*]

---

### Syntax Description

*command*

The name of the command.

---



---

### Usage Guidelines

Availability: *Remote*

If no command is specified, help information is displayed for all Group Configuration commands.

## info

Displays current information about the device group being created or edited.

**info**

---

### Usage Guidelines

Availability: *Remote*



# Configuration Command Set

Use Configuration mode commands to configure the Ethernet interface and SSL functions of the Secure Content Accelerator. Enter Configuration mode using the **enable** command in Non-Privileged mode and the **configure** command in Privileged mode. The prompt changes to `<config[devicename]>`.

## access-list

Adds an access list entry to the end of the specified access list. Use the **no** form of the command to delete the entire specified access list.

```
access-list <id> <permit | deny> <ipaddr> <mask>
no access-list <id>
```

### Syntax Description

<i>id</i>	The access list identifier.
<b>permit</b>	Allows access from the addresses specified in the list.
<b>deny</b>	Locks access from the addresses specified in the list.
<i>ipaddr</i>	The IP address to add to the specified list.
<i>mask</i>	The netmask appropriate to the IP address being added to the specified list.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

To activate the access list, you must also use the **remote-management access-list**, **snmp access-list**, **telnet access-list**, or **web-mgmt access-list** commands. A device can have up to 999 configured access lists.



**Note** Configuring an access list automatically sets up an implied access denial. For example, if you have set up an access list containing the IP addresses of remote hosts allowed to access the appliance, all other IP addresses have access denied. If you configure a single access list denying access from IP addresses in that list, all other IP addresses are denied access as well.



**Note** Access lists can be configured while the device is in FIPS Mode; however, they can only be assigned to the SNMP subsystem. Access lists can be assigned to other subsystems when the device is returned to normal operation.

---

## Examples

The following example specifies the host with the IP address 10.1.2.3 to be the only remote host to configure the Secure Content Accelerator.

```
access-list 2 permit 100.1.2.3 0.0.0.0
```

The following example specifies only remote hosts on the identified subnet can configure the Secure Content Accelerator.

```
access-list 1 permit 100.128.0.0 0.0.255.255
```

---

## Related Commands

**show access-list** (Privileged Command Set)  
**remote-management access-list** (Configuration Command Set)  
**snmp access-list** (Configuration Command Set)  
**telnet access-list** (Configuration Command Set)  
**web-mgmt access-list** (Configuration Command Set)

## clock

Allows the administrator to set the date or time.

**clock <date|time>**

---

**Syntax Description**

<b>date</b>	Sets the device date.
<b>time</b>	Sets the device time.

---

---

**Usage Guidelines**

Availability: *Serial; FIPS Mode (serial only)*

After entering the command, you are prompted to enter the appropriate date or time.

---

**Related Commands**

**show date** (Non-Privileged Command Set)

**show time** (Non-Privileged Command Set)

**end**

Leaves Configuration Mode and returns to Privileged Mode.

**end**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**exit**

Leaves Configuration Mode and returns to Privileged Mode.

**exit**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

<i>command</i>	The name of the command.
----------------	--------------------------

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Configuration commands

## hostname

Sets the identification name for the current Secure Content Accelerator.

**hostname** <*devname*>  
**no hostname**

---

### Syntax Description

<i>devname</i>	The name to assign to the current device.
----------------	---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to clear the hostname of the current device.



---

**Note** The command prompt reflects the new name the next time Configuration mode is entered.

---

## interface

Enters Interface Configuration mode for the specified Ethernet interface of the current device.

**interface <network|server>**

---

**Syntax Description**

<b>network</b>	Enters Interface Configuration Mode for the “Network” interface.
<b>server</b>	Enters Interface Configuration Mode for the “Server” interface.

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands**

**show interface** (Non-Privileged Command Set)  
**show interface errors** (Non-Privileged Command Set)  
**show interface statistics** (Non-Privileged Command Set)

See also “Interface Configuration Command Set”.

## ip address

Sets the IP address for the current Secure Content Accelerator.

```
ip address <<ipaddr> [netmask <netmask>]>|<ipaddr/netabbr>>
no ip address
```

Syntax Description		
	<i>ipaddr</i>	The IP address to assign to the device.
	<b>netmask</b> < <i>netmask</i> >	The netmask for the device.
	<i>netabbr</i>	The netmask abbreviation.

Usage Guidelines	
	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>
	If the netmask is not specified, a default value calculated from the user-provided IP address is used. Use the <b>no</b> form of the command to clear the IP address for the current device.

Related Commands	
	<b>ip route default</b> (Configuration Command Set)

## ip domain-name

Sets the default domain name for the device.

```
ip domain-name <name>
```

Syntax Description		
	<i>name</i>	The domain name.

Usage Guidelines	
	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>

**Related Commands**

- show ip domain-name** (Non-Privileged Command Set)
- show ip name-server** (Non-Privileged Command Set)
- ip name-server** (Configuration Command Set)

## ip name-server

Sets the one or more name servers to use with the device.

```
ip name-server <ipaddr>
```

Syntax Description	
<i>ipaddr</i>	The IP address of the Domain Name Server.

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

- show ip domain-name** (Non-Privileged Command Set)
- show ip name-server** (Non-Privileged Command Set)
- ip domain-name** (Configuration Command Set)

## ip route

Adds a static route entry for the specified destination IP address to the device routing table.

```
ip route <destip> <mask> <gatewayip> [metric <hops>]
no ip route <destip>
```

Syntax Description	
<i>destip</i>	The destination IP address.
<i>mask</i>	The netmask appropriate to the destination IP address.
<i>gatewayip</i>	The next-hop router address for the destination IP address.

<b>metric</b>	Specifies the total number of hops to the destination IP address
<i>hops</i>	The number of hops to the destination IP address.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to delete the specified static route entry from the device's routing table.

**Related Commands**

**show ip routes** (Non-Privileged Command Set)

**show route** (Non-Privileged Command Set)

## ip route default

Sets the default route for the current device.

**ip route default** *<ipaddr>*  
**no ip route default**

**Syntax Description**

<i>ipaddr</i>	The IP address of the default router to use.
---------------	--

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to clear the IP address for the default router.

**Related Commands**

**ip address** (Configuration Command Set)



## keepalive-monitor

Indicates that SSL errors from the specified IP address are to be ignored.

**keepalive-monitor** <ipaddr>  
**no keepalive-monitor** <ipaddr>

<b>Syntax Description</b>	<i>ipaddr</i>	The source IP address from which SSL errors are to be ignored.
---------------------------	---------------	--

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i> Up to two IP addresses, set individually, are allowed.
-------------------------	--

<b>Related Commands</b>	<b>show keepalive-monitor</b> (Non-Privileged Command Set)
-------------------------	--

## mode one-port

Enables secure and non-secure traffic to pass through the single “Network” Ethernet port. Use the **no** form of the command to return the device to dual-port mode.

**mode one-port**  
**no mode one-port**

<b>Usage Guidelines</b>	Availability: <i>Serial; FIPS Mode (serial only)</i> Use the <b>no</b> form of the command to clear the IP address.
-------------------------	--



<b>Note</b>	Though completers and help information are available in all management options, the command is only valid via serial management.
-------------	--

## mode pass-thru

Enables pass through of non-SSL traffic. This is the default configuration.

**mode pass-thru**  
**no mode pass-thru**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to block non-SSL traffic pass through.

## password

Sets the access- or enable-level password for the current Secure Content Accelerator.

**password <access|enable>**  
**no password <access|enable>**

### Syntax Description

<b>access</b>	Sets or clears the device attach-level password.
<b>enable</b>	Sets or clears the device enable-level password.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The access password is used when attaching to the device during a remote management session. You are prompted to enter and verify the password. Use the **no** form of the command to clear the access- or enable-level password for the current device.



#### Note

When using the **password** command in FIPS Mode, you must supply a password or passphrase of at least eight characters.

## rdate-server

Specifies and RDATE-protocol server to be used for date and time information on the device.

**rdate-server** <ipaddr>  
**no rdate-server**

---

<b>Syntax Description</b>	<i>ipaddr</i>	The IP address of the RDATE server.
---------------------------	---------------	-------------------------------------

---

---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--



---

<b>Note</b>	When a hostname is used rather than an IP address, the hostname is resolved as an IP address when written to the configuration.
-------------	---

---

---

<b>Related Commands</b>	<b>show date</b> (Non-Privileged Command Set) <b>show rdate-server</b> (Non-Privileged Command Set)
-------------------------	--

## registration-code

Stores the registration code of the device.

**registration-code** <code>

---

<b>Syntax Description</b>	<i>code</i>	The registration code of the device.
---------------------------	-------------	--------------------------------------

---

---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--

## remote-management access-list

Assigns the specified IP access list to the remote management subsystem.

**remote-management access-list** <id>  
**no remote-management access-list**

---

### Syntax Description

<i>id</i>	The identifier corresponding to an access list configured on the current device.
-----------	--

---



---

### Usage Guidelines

Availability: *Remote, Serial, Telnet*

Use the **no** form of the command to clear the IP access list assignment in the remote management subsystem. The access list still exists but is no longer used by the remote management subsystem.

---

### Related Commands

**access-list** (Configuration Command Set)  
**remote-management enable** (Configuration Command Set)  
**remote-management encryption** (Configuration Command Set)  
**remote-management port** (Configuration Command Set)  
**remote-management shared-secret** (Configuration Command Set)  
**show access-list** (Top Level Command Set)  
**show remote-management** (Non-Privileged Command Set)  
**telnet access-list** (Configuration Command Set)  
**web-mgmt access-list** (Configuration Command Set)

## remote-management enable

Enables remote management for the current device.

**remote-management enable**  
**no remote-management enable**

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet*Use the **no** form of the command to disable remote management of the current device.

---

**Note** Remote management is enabled by default.

---

---

**Related Commands**

**access-list** (Configuration Command Set)  
**remote-management access-list** (Configuration Command Set)  
**remote-management encryption** (Configuration Command Set)  
**remote-management port** (Configuration Command Set)  
**remote-management shared-secret** (Configuration Command Set)  
**show remote-management** (Non-Privileged Command Set)  
**telnet enable** (Configuration Command Set)  
**web-mgmt enable** (Configuration Command Set)

## remote-management encryption

Sets the encryption method for remote management sessions.

**remote-management encryption <ARC4|AES|DES>**

---

**Syntax Description**

<b>ARC4</b>	Sets the remote management encryption method to ARC4 (compatible with RC4™ RSA Data Security).
<b>AES</b>	Sets remote management encryption method to AES.
<b>DES</b>	Sets remote management encryption method to DES.

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet*Use this command after setting a passphrase using the **remote-management shared-secret** command. Encryption begins the next time the configuration manager accesses the Secure Content Accelerator.

<b>Related Commands</b>	<b>remote-management access-list</b> (Configuration Command Set) <b>remote-management enable</b> (Configuration Command Set) <b>remote-management port</b> (Configuration Command Set) <b>remote-management shared-secret</b> (Configuration Command Set) <b>show remote-management</b> (Non-Privileged Command Set)
-------------------------	--

## remote-management port

Sets the TCP service port used for remote management to the current device. Use the **no** form of the command to clear the port specification and return to the default communication port.

**remote-management port** <portid>  
**no remote-management port**

<b>Syntax Description</b>	<i>portid</i>	The TCP service port to be used to remotely manage the current device.
---------------------------	---------------	--

**Usage Guidelines**      Availability: *Remote, Serial, Telnet*

This port is used at the next attach. You must enter a **reload** command to activate the new remote management port.

<b>Related Commands</b>	<b>discover</b> (Non-Privileged Command Set) <b>remote-management access-list</b> (Configuration Command Set) <b>remote-management enable</b> (Configuration Command Set) <b>remote-management encryption</b> (Configuration Command Set) <b>remote-management shared-secret</b> (Configuration Command Set) <b>show remote-management</b> (Non-Privileged Command Set)
-------------------------	--

## remote-management shared-secret

Sets the secret passphrase used for encryption. Use the **no** form of the command to clear the passphrase.

**remote-management shared-secret** <passphrase>  
**no remote-management shared-secret**

### Syntax Description

<i>passphrase</i>	The passphrase used with encrypted management.
-------------------	--

### Usage Guidelines

Availability: *Serial*

You are prompted for this passphrase the next time a management connection with the device is requested.

### Related Commands

**remote-management access-list** (Configuration Command Set)  
**remote-management enable** (Configuration Command Set)  
**remote-management encryption** (Configuration Command Set)  
**remote-management port** (Configuration Command Set)  
**show remote-management** (Non-Privileged Command Set)

## rip

Enables Routing Interface Protocol (RIP) for the current device.

**rip** [v1|v2]  
**no rip** [v1|v2]

### Syntax Description

<b>v1</b>	Specifies RIP v1.
<b>v2</b>	Specifies RIP v2.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If a single RIP version is not specified, both versions are enabled. Using the **no** form of the command disables RIP completely if you do not specify a version to disable.

---

**Examples**

The following example activates RIP version 1. The first command enables both RIP versions. The second command disables on RIP v2. This has the same result as using the command **rip v1**.

```
rip
no rip v2
```

---

**Related Commands**

**show rip** (Non-Privileged Command Set)

## no snmp

Disables SNMP and clears all SNMP data.

**no snmp**

**Note**

---

The device must be rebooted (reloaded) before this command takes effect.

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands**

**show snmp** (Non-Privileged Command Set)  
**snmp access-list** (Non-Privileged Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp enable** (Configuration Command Set)  
**snmp location** (Configuration Command Set)



**snmp trap-host** (Configuration Command Set)  
**snmp trap-type enterprise** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)

## snmp access-list

Assigns an existing access list to be used with the SNMP subsystem.

**snmp access-list** <id>  
**no snmp access-list** <id>

### Syntax Description

<i>id</i>	The identifier corresponding to an access list configured on the current device.
-----------	--

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to remove the specified access list. The access list still exists but is no longer used by the SNMP subsystem.

### Related Commands

**access-list** (Configuration Command Set)  
**no snmp** (Configuration Command Set)  
**remote-management access-list** (Configuration Command Set)  
**show access-list** (Non-Privileged Command Set)  
**show snmp** (Non-Privileged Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp enable** (Configuration Command Set)  
**snmp location** (Configuration Command Set)  
**snmp trap-host** (Configuration Command Set)  
**snmp trap-type enterprise** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)  
**telnet access-list** (Configuration Command Set)  
**web-mgmt access-list** (Configuration Command Set)

## snmp contact

Assigns contact information for the SNMP subsystem. Use the **no** form of the command to remove the contact information.

```
snmp contact <contactInfo>
no snmp contact
```

<b>Syntax Description</b>	<i>contactInfo</i>	The string containing the contact information. Contact information must be entered within quotes.
---------------------------	--------------------	---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--

<b>Related Commands</b>	<p><b>no snmp</b> (Configuration Command Set)</p> <p><b>show snmp</b> (Non-Privileged Command Set)</p> <p><b>snmp access-list</b> (Configuration Command Set)</p> <p><b>snmp default community</b> (Configuration Command Set)</p> <p><b>snmp enable</b> (Configuration Command Set)</p> <p><b>snmp location</b> (Configuration Command Set)</p> <p><b>snmp trap-host</b> (Configuration Command Set)</p> <p><b>snmp trap-type enterprise</b> (Configuration Command Set)</p> <p><b>snmp trap-type generic</b> (Configuration Command Set)</p>
-------------------------	--

## snmp default community

Assigns a default community for the SNMP subsystem to use when sending trapping information.

```
snmp default community <comName>
no snmp default community
```

---

<b>Syntax Description</b>	<i>comName</i>	The string containing the community name. The string may contain up to 60 characters with no spaces. This information is not entered within quotes.
---------------------------	----------------	---

---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i> Use the <b>no</b> form of the command to clear the community name.	
-------------------------	--	--

---

<b>Related Commands</b>	<b>no snmp</b> (Configuration Command Set) <b>show snmp</b> (Non-Privileged Command Set) <b>snmp access-list</b> (Configuration Command Set) <b>snmp contact</b> (Configuration Command Set) <b>snmp enable</b> (Configuration Command Set) <b>snmp location</b> (Configuration Command Set) <b>snmp trap-host</b> (Configuration Command Set) <b>snmp trap-type enterprise</b> (Configuration Command Set) <b>snmp trap-type generic</b> (Configuration Command Set)	
-------------------------	---	--

## snmp enable

Enables SNMP using the current SNMP configuration.

**snmp enable**  
**no snmp enable**

---

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i> Use the <b>no</b> form of the command to disable SNMP without clearing SNMP data.
-------------------------	---

**Note**

---

The device must be rebooted (reloaded) before this command takes effect.

---

**Related Commands**

**show snmp** (Non-Privileged Command Set)  
**snmp access-list** (Configuration Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp location** (Configuration Command Set)  
**snmp trap-host** (Configuration Command Set)  
**snmp trap-type enterprise** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)

## snmp location

Assigns location information for the SNMP subsystem.

**snmp location** <*locInfo*>  
**no snmp location**

**Syntax Description**

<i>locInfo</i>	The string containing the location information. This information is entered within quotes.
----------------	--

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to clear the location information.

**Related Commands**

**no snmp** (Configuration Command Set)  
**show snmp** (Non-Privileged Command Set)  
**snmp access-list** (Configuration Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp enable** (Configuration Command Set)  
**snmp trap-host** (Configuration Command Set)  
**snmp trap-type enterprise** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)

## snmp trap-host

Assigns a destination for SNMP trap messages.

```
snmp trap-host <v1|v2c> <ipaddr> [community]
no snmp trap-host <v1|v2c> <ipaddr> [community]
```

### Syntax Description

<b>v1</b>	Specifies SNMP version 1.
<b>v2c</b>	Specifies SNMP version 2c.
<i>ipaddr</i>	The IP address of the computer receiving the messages.
<i>community</i>	The SNMP community. If a community is specified with the <b>snmp default community</b> command, you do not need to specify a community with this command. If you wish trap messages to be sent to a community <i>other</i> than the default community, you must specify a community when giving this command.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### Related Commands

- no snmp** (Configuration Command Set)
- show snmp** (Non-Privileged Command Set)
- snmp access-list** (Configuration Command Set)
- snmp contact** (Configuration Command Set)
- snmp default community** (Configuration Command Set)
- snmp enable** (Configuration Command Set)
- snmp location** (Configuration Command Set)
- snmp trap-type enterprise** (Configuration Command Set)
- snmp trap-type generic** (Configuration Command Set)

## snmp trap-type enterprise

Enables device event trap messages to be sent for a specific trap-type event and event filter.

```
snmp trap-type enterprise <config-changed|cpu-utilization|
ssl-cert-expire|ssl-cert-invalid|ssl-certify-fail|
ssl-neg-failure|ssl-total-connections|ssl-tps> [threshold <threshold>]
[hysteresis <lowvalue> <highvalue>]
no snmp trap-type enterprise <config-changed|cpu-utilization|
ssl-cert-expire|ssl-cert-invalid|ssl-certify-fail|
ssl-neg-failure|ssl-total-connections|ssl-tps>
```

Syntax Description		
	<b>config-changed</b>	Specifies trapping for device configuration changes.
	<b>cpu-utilization</b>	Specifies trapping for CPU utilization levels.
	<b>ssl-total-connections</b>	Specifies trapping for total SSL connection levels.
	<b>ssl-tps</b>	Specifies trapping for SSL transactions per second levels.
	<b>threshold</b> <value1> [<value2>]	Specifies the <b>threshold</b> option to specify one or more threshold levels, where appropriate. (Threshold values are inappropriate for the <b>config-changed</b> option.) Threshold <i>value1</i> is the low level and optional threshold <i>value2</i> is the high level. Values must be entered as integers and are inclusive. A device is considered to be at a low level until the high level value ( <i>value2</i> ) is exceeded; a device is considered to be at a high level until it reaches or exceeds the low level value ( <i>value1</i> ). If no threshold values are specified, the default values are used. If only one threshold value is specified, it is used as both the high and low level value; otherwise, two-level thresholding behavior occurs using the default or user-specified levels for each value.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

(This command must be entered on one line.) Use the **no** form of the command to disable the specified event trap-type. The table below shows trap-type minimum, maximum, and default levels for each value argument. Except in the case of **cpu-utilization**, the levels indicate actual values; **cpu-utilization** levels indicate percentage of use.

Trap-Type	Value1 Min	Value1 Max	Value1 Default	Value2 Min	Value2 Max	Value2 Default
cpu-utilization	1	99	75	1	99	90
ssl-tps	1	2500	170	1	2500	190
ssl-total-connections	1	10000	600	1	10000	800

### Related Commands

**no snmp** (Configuration Command Set)  
**show snmp** (Top Level Command Set)  
**snmp access-list** (Configuration Command Set)  
**snmp contact** (Configuration Command Set)  
**snmp default community** (Configuration Command Set)  
**snmp enable** (Configuration Command Set)  
**snmp location** (Configuration Command Set)  
**snmp trap-host** (Configuration Command Set)  
**snmp trap-type generic** (Configuration Command Set)

## snmp trap-type generic

Enables generic SNMP traps.

**snmp trap-type generic**  
**no snmp trap-type generic**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to disable generic SNMP traps.

<b>Related Commands</b>	<b>no snmp</b> (Configuration Command Set) <b>show snmp</b> (Non-Privileged Command Set) <b>snmp access-list</b> (Configuration Command Set) <b>snmp contact</b> (Configuration Command Set) <b>snmp default community</b> (Configuration Command Set) <b>snmp enable</b> (Configuration Command Set) <b>snmp location</b> (Configuration Command Set) <b>snmp trap-host</b> (Configuration Command Set) <b>snmp trap-type enterprise</b> (Configuration Command Set)
-------------------------	---

## sntp interval

Sets polling interval for all configured SNMP servers.

**sntp interval** <*seconds*>

<b>Syntax Description</b>	<i>seconds</i>	The number of seconds between polls.
---------------------------	----------------	--------------------------------------

<b>Usage Guidelines</b>	Availability: <i>Remote, Serial, Telnet; FIPS Mode (serial only)</i>
-------------------------	--

The default interval is 86400 seconds (one day), the minimum and maximum intervals are 60 and 2419200 (one month), respectively. The interval can be displayed using the commands **show device**, **show sntp** and **write terminal**.

<b>Related Commands</b>	<b>show device</b> (Non-Privileged Command Set) <b>show sntp</b> (Non-Privileged Command Set) <b>sntp server</b> (Configuration Command Set) <b>write terminal</b> (Privileged Command Set)
-------------------------	--

## sntp server

Assigns an SNMP server.



**sntp server** <ipaddr>  
**no sntp server** <ipaddr>

---

**Syntax Description**

---

*ipaddr* The IP address of the SNTP server.

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

You are prompted to enter and verify the password. Use the **no** form of the command to clear the SNTP server. If more than one SNTP server has been configured, you must specify the IP address or hostname of the one to delete. Up to four SNTP servers can be configured. If the first SNTP server returns an error, the next SNTP server is polled. After the fourth SNTP poll returns an error, the first server is polled again. SNTP information can be displayed using the commands **show device**, **show sntp** and **write terminal**.



---

**Note** When a hostname is used rather than an IP address, the hostname is resolved as an IP address when written to the configuration.

---

---

**Related Commands**

**show device** (Non-Privileged Command Set)  
**show sntp** (Non-Privileged Command Set)  
**sntp interval** (Configuration Command Set)  
**write terminal** (Privileged Command Set)

## ssl

Enters SSL Configuration mode for the current device.

**ssl**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl errors** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)  
**show ssl statistics** (Non-Privileged Command Set)

See the section “SSL Configuration Command Set”.

## syslog

Adds the specified IP address to the syslog list for the device.

```

syslog <ipaddr>
no syslog <ipaddr>
  
```

**Syntax Description**

<i>ipaddr</i>	The IP address of the device to receive syslog messages.
---------------	--

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Using the **no** form of the command removes the specified IP address from the syslog list of the current device. Up to four IP addresses can be specified. Syslog messages are sent to all hosts at the IP addresses in this list.

**Related Commands**

**show syslog** (Non-Privileged Command Set)

## telnet access-list

Assigns an existing access list to be used with telnet management requests.

**telnet access-list <id>**  
**no telnet access-list <id>**

---

<b>Syntax Description</b>	<i>id</i>	The identifier corresponding to an access list configured on the current device.
---------------------------	-----------	--

---

---

<b>Usage Guidelines</b>	<i>Availability: Remote, Serial, Telnet</i>
-------------------------	---

Use the **no** form of the command to remove the specified access list. The access list still exists but is no longer used by the telnet subsystem.

---

<b>Related Commands</b>	<b>access-list</b> (Configuration Command Set) <b>remote-management access-list</b> (Configuration Command Set) <b>show telnet</b> (Non-Privileged Command Set) <b>telnet enable</b> (Configuration Command Set) <b>telnet port</b> (Configuration Command Set) <b>web-mgmt access-list</b> (Configuration Command Set)
-------------------------	--

## telnet enable

Allows telnet management sessions for the device. Use the **no** form of the command to disable telnet management access.

**telnet enable**  
**no telnet enable**

---

<b>Usage Guidelines</b>	<i>Availability: Remote, Serial, Telnet</i>
-------------------------	---

---

<b>Related Commands</b>	<b>show telnet</b> (Non-Privileged Command Set) <b>telnet access-list</b> (Configuration Command Set) <b>telnet port</b> (Configuration Command Set)
-------------------------	--

## telnet port

Specifies the TCP service port to use for telnet management sessions.

**telnet port** <portid>  
**no telnet port** <portid>

Syntax Description	<i>portid</i>	The TCP service port to be used to manage the current device via a telnet session.
--------------------	---------------	--

Usage Guidelines;	Availability: <i>Remote, Serial, Telnet</i>
	Use the <b>no</b> form of the command to return the telnet management port to the default setting. The port assignment is used at the next attach.

Related Commands	<b>show telnet</b> (Non-Privileged Command Set) <b>telnet access-list</b> (Configuration Command Set) <b>telnet enable</b> (Configuration Command Set)
------------------	--

## timezone

Specifies the time zone of the device's location.

**timezone** <zone>

Syntax Description	<i>zone</i>	The time zone identifier.
--------------------	-------------	---------------------------

Usage Guidelines	Availability: <i>Serial, Telnet; FIPS Mode (serial only)</i>
------------------	--

The *zone* is entered in the form of Standard Time Zone identifier|GMT offset (integer)|Daylight Savings Time Zone identifier. For example, MST7MDT is used for Mountain Standard/Daylight Savings Time. The alphabetic strings are used for display; the integer is used for date and time computation. The alphabetic strings are optional; the GMT offset integer is not.

**Related Commands**    **show date** (Non-Privileged Command Set)

## web-mgmt access-list

Assigns an existing access list to be used with web browser-based management requests.

```
web-mgmt access-list <id>
no web-mgmt access-list <id>
```

Syntax Description	<i>id</i>
	The identifier corresponding to an access list configured on the current device.

**Usage Guidelines**    Availability: *Remote, Serial, Telnet*

Use the **no** form of the command to remove the specified access list. The access-list still exists but is no longer used by the Web management subsystem.

**Related Commands**    **access-list** (Configuration Command Set)  
**remote-management access-list** (Configuration Command Set)  
**show web-management** (Non-Privileged Command Set)  
**telnet access-list** (Configuration Command Set)  
**web-mgmt enable** (Configuration Command Set)  
**web-mgmt port** (Configuration Command Set)

## web-mgmt enable

Allows web browser-based management sessions for the device. Use the **no** form of the command to diable web browser-based management access.

**web-mgmt enable**  
**no web-mgmt enable**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet*

---

### Related Commands

**show web-management** (Non-Privileged Command Set)  
**web-mgmt access-list** (Configuration Command Set)  
**web-mgmt port** (Configuration Command Set)

## web-mgmt port

Specifies the TCP service port used for management with the Web-based GUI.

**web-mgmt port** *<portid>*  
**no web-mgmt port** *<portid>*

---

### Syntax Description

<i>portid</i>	The TCP service port to be used to manage the current device via the GUI.
---------------	---

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet*

Use the **no** form of the command to return the GUI management port to the default setting. The port assignment is used at the next attach.

---

**Related Commands**

**access-list** (Configuration Command Set)  
**show web-management** (Non-Privileged Command Set)  
**web-mgmt access-list** (Configuration Command Set)  
**web-mgmt enable** (Configuration Command Set)

## Interface Configuration Command Set

Use these commands to manage the speed and duplex settings of the specified Ethernet interface on the current Secure Content Accelerator. Enter Interface Configuration mode by using the **enable** command in Non-Privileged mode and the **configure** command in Privileged mode. Specify an Ethernet interface to configure using the **interface** command in Configuration mode. The prompt changes to `<config-if[interfacename]>>`.

### auto

Sets the current Ethernet interface to autonegotiation, canceling any existing forced duplex or speed setting.

**auto**

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### duplex

Forces the current Ethernet interface to full or half duplex.

**duplex <full|half>**

#### Syntax Description

<b>full</b>	Sets the current interface to full duplex.
<b>half</b>	Sets the current interface to half duplex.

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### end

Exits Interface Configuration mode and returns to Configuration mode.

**end**



## finished

Leaves Interface Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

<i>command</i>	The name of the command.
----------------	--------------------------

---



---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Interface Commands

## speed

Forces the speed of the current Ethernet interface to 10 Mbps or 100 Mbps.

**speed** <10|100>

---

### Syntax Description

<b>10</b>	Sets the current interface speed to 10 Mbps.
<b>100</b>	Sets the current interface speed to 100 Mbps.

---



---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## SSL Configuration Command Set

Use these commands to set up and manage the SSL configuration for the current Secure Content Accelerator. Enter the SSL Configuration mode by using the **enable** command in the Non-Privileged Mode, **configure** command in the Privileged Mode, and the **ssl** command in Configuration Mode. The prompt changes to `<config-ssl[devicename]>>`.

### backend-server

Creates and/or configures the specified backend server and enters Backend Server Configuration mode for that server.

```
backend-server <servname> [create]
no backend-server <servname>
```

#### Syntax Description

<i>servname</i>	The name of the backend server.
<b>create</b>	Creates a new backend server named <i>servname</i> and enters Backend Server Configuration mode for that object.

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove the specified backend server. A device can have a total of 255 servers in any combination of backend, reverse-proxy, or standard secure servers. When a backend server has been specified for removal, all connections are allowed to finish before the backend server is actually removed. Backend server names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Backend server names must begin with an alphabetic character or underscore and have a limit of 15 characters.

#### Related Commands

**show ssl** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)

See the section “Backend Server Configuration Command Set”.

## cert

Creates and/or configures the specified certificate object and enters Certificate configuration mode for that object.

```
cert <certname> [create]  
no cert <certname>
```

Syntax Description		
	<i>certname</i>	The name of the certificate object.
	<b>create</b>	Creates a new certificate object named <i>certname</i> and enters Certificate Configuration mode for that object.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove the specified certificate object. You cannot remove a certificate referenced by a server. A device can have up to 511 certificate objects. Certificate names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Certificate names must begin with an alphabetic character or underscore and have a limit of 127 characters.

### Examples

The following example creates a certificate object named *myCert* and enters Certificate Configuration mode for the certificate object *myCert*.

```
cert myCert create
```

### Related Commands

**show ssl cert** (Non-Privileged Command Set)

See the section “Certificate Configuration Command Set”.

## certgroup

Creates and/or configures the specified certificate group and enters Certificate Group Configuration mode for the certificate group.

```
certgroup <certgroupname> [create]
no certgroup <certgroupname>
```

### Syntax Description

<i>certgroupname</i>	The name of the certificate group.
<b>create</b>	Creates a new certificate group named <i>certgroupname</i> and enters Certificate Group Configuration mode for that object.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove the specified certificate group. You cannot remove a certificate group referenced by a server. A device can have up to 63 certificate groups. Certificate group names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Certificate group names must begin with an alphabetic character or underscore and have a limit of 15 characters.

### Examples

The following example creates a certificate object named *myCertGroup* and enters Certificate Group Configuration mode for certificate group *myCertGroup*.

```
cert myCertGroup create
```

### Related Commands

**show ssl certgroup** (Top Level Command Set)

See the section “Certificate Group Configuration Command Set”.

## end

Exits SSL Configuration mode and returns to Configuration mode.

**end**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves SSL Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## gencsr

Generates a certificate signing request and/or self-signed certificate.

**gencsr** <key <keyname>> [**newhdr**] [**digest md5|sha1**] [**output** <filename|url>]

---

### Syntax Description

<i>keyname</i>	The name of the key generated.
<b>newhdr</b>	Inserts the word “NEW” into the CSR header. This is required by some older CAs.
<b>digest</b>	Displays a digest form of the certificate.
<b>md5</b>	Displays a digest form of the certificate in MD5 format.
<b>sha1</b>	Displays a digest form of the certificate in SHA1 format.
<b>output</b>	Outputs the certificate file for backup purposes.

<i>filename</i>	The name of the certificate file.
<i>url</i>	The location of the certificate file (serial and telnet only).

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

A device can up to 255 key objects.

**Examples**

The following example uses a key object named *myGenKey*, displays the certificate digest in MD5 format, and saves the certificate file named *myCertFile*.

```
gencsr key myGenKey digest md5 output myCertFile
```

**Related Commands**

See the section “Key Configuration Command Set”.

**help**

Displays help information for the specified command.

**help** [*command*]

**Syntax Description**

<i>command</i>	The name of the command.
----------------	--------------------------

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all SSL Commands

## import pkcs12

Imports and processes a PKCS#12 file to create certificate and key objects.

```
import pkcs12 <name> [filename/url]
```

Syntax Description		
	<i>name</i>	The user-defined name for the certificate and key objects.
	<i>filename</i>	The path and name of the file on the local file system.
	<i>url</i>	The location of the file (serial and telnet only).

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a file name or URL, you are prompted for it.

### Related Commands

**import pkcs7** (SSL Command Set)  
**show ssl cert** (Non-Privileged Command Set)  
**show ssl key** (Non-Privileged Command Set)

## import pkcs7

Imports and processes a PKCS#7 file to create a certificate objects and a certificate group.

```
import pkcs7 <name> <der|pem> [prefix <prefixText>] [filename][url]
```

Syntax Description		
	<i>name</i>	The user-defined name of the certificate group object.
	<b>der</b>	Indicates the file is DER-encoded.
	<b>pem</b>	Indicates the file is PEM-encoded.
	<b>prefix</b>	Indicates a prefix should be used when naming certificate objects.
	<i>prefixText</i>	The prefix used for the certificate names in the chain.

<i>filename</i>	The path and name of the file on the local file system.
<i>url</i>	The location of the file (serial and telnet only).

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a file name or URL, you are prompted for it.

**Related Commands**

**import pkcs12** (SSL Command Set)

**show ssl cert** (Non-Privileged Command Set)

**show ssl certgroup** (Non-Privileged Command Set)

**key**

Creates and/or configures the specified key object.

**key** <keyname> [**create**]  
**no key** <keyname>

**Syntax Description**

<i>keyname</i>	The name of the key.
<b>create</b>	Creates a new key association named <i>keyname</i> and enters Key Configuration mode for that object.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove a key. You cannot delete a key referenced by a server. A device can have up to 255 key objects. Key names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Key names must begin with an alphabetic character or underscore and have a limit of 15 characters.



---

**Examples**

The following example creates a key association named *mykey* and enters Key Configuration mode for the key association *mykey*.

```
key mykey create
```

---

**Related Commands**

**show ssl key** (Non-Privileged Command Set)

See the section “Key Configuration Command Set”.

---

**reverse-proxy-server**

Creates and/or configures the specified reverse-proxy server and enters Reverse-Proxy Server Configuration mode for that server.

```
reverse-proxy-server <servname> [create]
no reverse-proxy-server <servname>
```

---

**Syntax Description**

<i>servname</i>	The name of the reverse-proxy server.
<b>create</b>	Creates a new reverse-proxy server named <i>servname</i> and enters Reverse-Proxy Server Configuration mode for that object.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove the specified reverse-proxy server. A device can have a total of 255 servers in any combination of backend, reverse-proxy, or standard secure servers. When a reverse-proxy server has been specified for removal, all connections are allowed to finish before the reverse-proxy server is actually removed. Reverse-proxy server names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Reverse-proxy server names must begin with an alphabetic character or underscore and have a limit of 15 characters.

**Related Commands**

**show ssl** (Non-Privileged Command Set)  
**show ssl server** (Non-Privileged Command Set)

See the section “Reverse-Proxy Server Configuration Command Set”.

**secpolicy**

Creates and/or configures the specified security policy and enters Security Policy Configuration mode for the security policy.

**secpolicy** <polname> [**create**]  
**no secpolicy** <polname>

**Syntax Description**

<i>polname</i>	The name of the security policy.
<b>create</b>	Creates a new security policy named <i>polname</i> and enters Security Policy Configuration mode for that object.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove a security policy. You cannot delete a security policy referenced by a logical secure server. Security policy names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Security policy names must begin with an alphabetic character or underscore and have a limit of 15 characters.

**Examples**

The following example creates a security policy named *mypolicy* and enters Security Policy Configuration mode for the security policy *mypolicy*.

```
secpolicy mypolicy create
```

**Related Commands**

**show ssl secpolicy** (Non-Privileged Command Set)

See the section “Security Policy Configuration Command Set”.

## server

Creates and/or configures the specified standard secure server and enters Server Configuration mode for that server.

```
server <servname> [create]
no server <servname>
```

### Syntax Description

<i>servname</i>	The name of the logical secure server.
<b>create</b>	Creates a new logical secure server named <i>polname</i> and enters Server Configuration mode for that server.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to remove a server. A device can have a total of 255 servers in any combination of backend, reverse-proxy, or standard secure servers. When a secure server has been specified for removal, all connections are finished before the server is actually removed. Server names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore (\_), hyphen (-), and period (.) characters. Server names must begin with an alphabetic character or underscore and have a limit of 15 characters.

### Related Commands

**show ssl server** (Non-Privileged Command Set)

See the section “Server Configuration Command Set”.

## Backend Server Configuration Command Set

Use Backend Server Configuration commands to set up and configure backend servers. Enter Backend Server Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged mode, the **ssl** command in Configuration mode, and the **backend-server** command in SSL Configuration mode. The prompt changes to `<config-ssl-backend[servername]>>`.

### activate

Activates the current suspended backend server if enough information has been configured.

**activate**

---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

All backend servers are created as active servers by default.

---

#### Related Commands

**suspend** (Backend Server Configuration Command Set)

### certgroup serverauth

Assigns a certificate group to be used for server certificate authentication.

**certgroup serverauth** *<certgroupname>*  
**no certgroupchain**

---

#### Syntax Description

<i>certgroupname</i>	The name of the certificate group.
----------------------	------------------------------------

---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to disable server authentication using the certificate group. When using the **no** form of the command, you need not specify any certificate group name. Only one certificate group can be used.

---

**Related Commands**

**certgroup** (SSL Configuration Command Set)  
**show ssl certgroup** (Non-Privileged Command Set)

See also “Certificate Group Configuration Command Set”.

**end**

Exits Backend Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**end**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**exit**

Exits Backend Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**finished**

Leaves Backend Server Configuration Mode and returns to Top Level mode.

**finished**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

<i>command</i>	The name of the command.
----------------	--------------------------

---



---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Backend Server Configuration Commands.

## info

Displays current information about the logical secure server being edited or created.

**info**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## ip address

Sets the specified IP address for the backend server.

**ip address** <*ipaddr*> [**netmask** <*mask*>]  
**no ip address**

---

### Syntax Description

<i>ipaddr</i>	The IP address to assign to the backend server.
<b>netmask</b> < <i>mask</i> >	The netmask valid for the IP address.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Using the **no** form of the command clears the IP address for the backend server.

**localport**

Specifies the TCP service port through which non-secure connections are received.

**localport** <port|default>

**Syntax Description**

<i>port</i>	The used to transfer non-secure traffic.
<b>default</b>	Sets the port specification to 80.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**remoteport** (Backend Server Configuration Command Set)

**log-url**

Specifies a host for logging of URL requests.

**log-url** <ipaddr>

**Syntax Description**

<i>ipaddr</i>	The IP address of the host for the log.
---------------	---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## remoteport

Specifies the TCP service port through which redirected secure connections are sent.

**remoteport** <*port*|**default**>

<b>Syntax Description</b>	<i>port</i>	The used to transfer secure traffic.
	<b>default</b>	Sets the port specification to 443.



### Caution

Traffic sent on this TCP service port is not secured by SSL during transmission to the server. It must be secured by another means.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### Related Commands

**localport** (Backend Server Configuration Command Set)

## secpolicy

Creates an association between this server and the specified security policy.

**secpolicy** <*polname*|**all**|**default**|**fips**|**noexport56**|**strong**|**weak**>

<b>Syntax Description</b>	<i>polname</i>	The name of the configured security policy.
	<b>all</b>	All pre-loaded security policies.
	<b>default</b>	Default security policy set.
	<b>fips</b>	FIPS 104-2-compliant security policy set.



<b>noexport56</b>	Security policy set used to address potential problems in non-US installations using Internet Explorer. While this security policy disables the 56-bit cipher suite, it does not compromise the strength or the integrity of the encryption in any way.
<b>strong</b>	Strong security policy set.
<b>weak</b>	Weak security policy set.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Several default security policies are preloaded into the SSL device. To see a list of all loaded default and user-defined security policies, use the **show ssl secpolicy** command.

### Related Commands

**secpolicy** (SSL Configuration Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)

See the section “Security Policy Configuration Command Set”.

## serverauth enable

Enables server certificate authentication.

**serverauth enable**  
**no serverauth enable**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Using the **no** form of the command disables server certificate authentication.

### Related Commands

**certgroup serverauth** (Backend Server Configuration Command Set)  
**serverauth ignore** (Backend Server Configuration Command Set)

## serverauth ignore

Specifies the server authentication errors to ignore.

```
serverauth ignore all | none|signature-failure|expired-date|
cert-not-yet-valid|invalid-ca|domain-name
no serverauth ignore all | none|signature-failure|expired-date|
cert-not-yet-valid|invalid-ca|domain-name
```

Syntax Description		
<b>all</b>	Ignore all server authentication errors.	
<b>non</b>	Do not ignore server authentication errors.	
<b>signature-failure</b>	Ignore certificate signature failure errors.	
<b>expired-date</b>	Ignore certificate expiration errors.	
<b>cert-not-yet-valid</b>	Ignore errors caused by using the certificate before it is valid.	
<b>invalid-ca</b>	Ignore errors caused by an unrecognized CA.	
<b>domain-name</b>	Ignore errors due to an invalid domain name.	

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Any combination of options can be used currently. Use the **no** form of the command to cease ignoring the specific server authentication error.

### Related Commands

**certgroup serverauth** (Backend Server Configuration Command Set)  
**serverauth enable** (Backend Server Configuration Command Set)

## session-cache enable

Enables session caching.

```
session-cache enable
no session-cache enable
```

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*Use the **no** form of the command to disable session caching.

---

**Related Commands****session-cache size** (Backend Server Configuration Mode)**session-cache timeout** (Backend Server Configuration Mode)

## session-cache size

Specifies the size of the session cache.

**session-cache size** <cache-size>

---

**Syntax Description***cache-size*

The number of sessions to be cached. The default is 1024. The acceptable range is 1 to 76,800.

---

**Usage Guidelines**Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands****session-cache enable** (Backend Server Configuration Mode)**session-cache timeout** (Backend Server Configuration Mode)

## session-cache timeout

Specifies the session cache length before being timed out.

**session-cache timeout** <seconds>

---

**Syntax Description***seconds*

Specifies the number of seconds before the cache times out.

---

**Usage Guidelines**      Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands**      **session-cache enable** (Backend Server Configuration Mode)  
**session-cache size** (Backend Server Configuration Mode)

## suspend

Suspends the function of the backend server.

**suspend [now]**

---

**Syntax Description**      **now**      Suspends actions of the backend server immediately.

---

---

**Usage Guidelines**      Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

This command behaves in three ways:

- If you are creating a new backend server and you use the **suspend** command, the server is created in the suspended state. No connections are accepted until the **activate** command is used.
- If you are editing an existing backend server and you use the **suspend** command alone, the all open connections on the server are finished, and no new connections are accepted. No connections are accepted until the **activate** command is used.
- If you are editing an existing backend server and you use the **suspend now** command, all connections are suspended. When the **end** command is entered, the current backend server is removed, and a new suspended backend server is created.

---

**Related Commands**      **activate** (Backend Server Configuration Mode)

## transparent

Enables the backend server to function as a transparent proxy (default).

**transparent**  
**no transparent**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When transparent proxy behavior is disabled, the device accepts connections on the IP address of the Secure Content Accelerator rather than on the server address. The **no** form of the command is used to disable this behavior.

## urlrewrite

Sets or remove a specified URL rewrite rule for the current backend server.

**urlrewrite** *<domainName>* [**sslport** *<portid>*] [**clearport** *<portid>*]  
*<redirectonly>*  
**no urlrewrite** *<domainName>*

### Syntax Description

<i>domainName</i>	The domain or file identifier as a domain name, IP address, or path and file name.
<b>sslport</b>	A keyword identifying the following <i>portid</i> to be used for SSL traffic.
<i>portid</i>	The TCP service port to be used for SSL traffic.
<b>clearport</b>	A keyword identifying the following <i>portid</i> to be used for clear text traffic.
<i>portid</i>	The TCP service port to be used for clear text traffic.
<b>redirectonly</b>	A keyword is used to indicate that only the “Location;” field in the HTTP 30x redirect header should be rewritten. This solves a common problem with Web servers using insecure HTTP 30x redirects.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

An \* (asterisk) wild card character can be used to specify more than one server in a single domain, e.g., “\*.company.com”. Up to 32 URL rewrite rules can be configured. Use the **no** form of the command to clear the specified rule. If more than one rule has been configured, you must specify the domain name of the rule to delete. URL rewrite information can be displayed by using the command **show ssl server**.

---

**Related Commands**

**show ssl server** (Non-Privileged Command Set)

## Certificate Configuration Command Set

Use Certificate Configuration commands to set up and manage certificate objects. Enter Certificate Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged Mode, the **ssl** command in Configuration mode, and the **cert** command in SSL Configuration mode. The prompt changes to `<config-ssl-cert[certname]>>`.

### binhex

Pastes a binary hex-encoded X509 certificate into the configuration manager.

**binhex** [*value*]

#### Syntax Description

<i>value</i>	The certificate that has been copied into the cut buffer.
--------------	---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

After the command is entered, you are prompted to paste the certificate from the cut buffer. You can use a text editor to copy the certificate from a file. After the certificate is pasted, you must press **Enter** twice to complete the command.

### der

Loads a DER-encoded X509 certificate file into the current object.

**der** [*certfilename*|*url*]

#### Syntax Description

<i>certfilename</i>	The name of the DER-encoded certificate file.
<i>url</i>	The location of the file (serial and telnet only).

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not enter the file name or URL, you are prompted for it.

## end

Exits Certificate Configuration mode, activates all valid changes, and returns to SSL Configuration mode.

**end**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## exit

Exits Certificate Configuration mode, activates all valid changes, and returns to SSL Configuration mode.

**exit**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Certificate Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

<i>command</i>	The name of the command.
----------------	--------------------------



**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Certificate Configuration Commands

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**info**

Displays current information about the certificate object being created or edited.

**info**

**pem**

Loads a PEM-encoded X509 certificate into the current certificate object.

**pem** [*certfilename*]*|url*

**Syntax Description**

<i>certfilename</i>	The name of the PEM-encoded certificate file.
<i>url</i>	The location of the file (serial and telnet only).

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not enter the file name or URL, you are prompted for it.

**Related Commands**

**pem-paste** (Certificate Configuration Command Set)

**pem-paste**

Allows a PEM-encoded X.509 certificate to be pasted into the configuration manager.

**pem-paste**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

After the command is entered, you are prompted to paste a certificate from the cut buffer. You can use a text editor to copy the certificate from a file. After the certificate is pasted, you must press **Enter** twice to complete the command.

---

**Related Commands**

**pem** (Certificate Configuration Command Set)

## Certificate Group Configuration Command Set

Use Certificate Group Configuration commands to set up and manage certificate groups utilized for certificate chains and server and client certificate authentication. Enter Certificate Group Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged mode, the **ssl** command in Configuration mode, and the **certgroup** command in SSL Configuration mode. The prompt changes to `<config-ssl-certgroup[certgroupname]>>`.

### cert

Adds the specified, existing certificate object into the current certificate group.

```
cert <certObject>
no cert <certObject>
```

#### Syntax Description

<i>certObject</i>	The name of the certificate object.
-------------------	-------------------------------------

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Up to 64 certificate objects are allowed per certificate group. Use the **no** form of the command to remove the specified certificate from the certificate group.

#### Related Commands

**cert** (SSL Configuration Command Set)

See the section “Certificate Configuration Command Set”.

### end

Exits Certificate Group Configuration mode, activates all changes, and returns to SSL Configuration mode.

```
end
```

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## exit

Exits Certificate Group Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Certificate Group Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

---

<i>command</i>	The name of the command.
----------------	--------------------------

---

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Certificate Group Commands

## info

Displays current information about the certificate group being created or edited.

### info

---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## Key Configuration Command Set

Use Key Configuration commands to set up and manage keys. Enter Key Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged mode, the **ssl** command in Configuration mode, and the **key** command in SSL Configuration mode. The prompt changes to `<config-ssl-key[keyname]>>`.

### binhex

Allows a binary hex-encoded X.509 key to be pasted into the configuration manager.

**binhex** [*value*]

#### Syntax Description

<i>value</i>	The key that has been copied into the cut buffer.
--------------	---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

After the command is entered, you are prompted to paste the key from the cut buffer. You can use a text editor to copy the key from a file. After the key is pasted, you must press **Enter** twice to complete the command.

### der

Loads a DER-encoded X509 key file into the current key object.

**der** [*keyfilename*]*|url*]

#### Syntax Description

<i>keyfilename</i>	The name of the DER-encoded key file.
<i>url</i>	The location of the file (serial and telnet only).

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not enter the file name or URL, you are prompted for it.

## end

Exits Key Configuration mode, activates all changes, and returns to SSL Configuration mode.

**end**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## exit

Exits Key Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Key Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## genrsa

Generates an RSA key.

**genrsa [bits <512|1024>] [encrypt <des|des3>] [seed <seedstring>]  
[output <filename/url>]**

<b>Syntax Description</b>	<b>bits</b>	Specifies the key strength.
	<b>512</b>	Specifies the key to be 512-bit strength.
	<b>1024</b>	Specifies the key to be 1024-bit strength.
	<b>encrypt</b>	Encrypts the generated key for display.
	<b>des</b>	Specifies DES to be used for the encrypted key displayed.
	<b>des3</b>	Specifies DES3 to be used for the encrypted key displayed.
	<b>seed</b>	Specifies a seed string to be used for key generation.
	<i>seedstring</i>	The string used to generate the key.
	<b>output</b>	Writes the PEM-encoded key file to disk.
	<i>filename</i>	The name of the PEM-encoded key file.
	<i>url</i>	The location of the file (serial and telnet only).

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If the **encrypt** keyword is not used, the key is not be displayed.

**Examples**

The following example generates a 1024-bit key using the seed string *lemon*. The key is displayed once using DES encryption. The resulting key is stored on the device as well as exported to a PEM-encoded file named *mykey.pem*.

```
genrsa bits 1024 encrypt des seed lemon output mykey.pem
```

**help**

Displays help information for the specified command.

**help** [*command*]

**Syntax Description**

<i>command</i>	The name of the command.
----------------	--------------------------



**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Key Configuration Commands

**info**

Displays current information about the key being created or edited.

**info****Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**net-iis**

Loads a private key exported from IIS 4 only into the key entity.

**net-iis** [*keyfilename|url*]

**Syntax Description**

<i>key-filename</i>	The name of the key file.
<i>url</i>	The location of the file (serial and telnet only).

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not enter the file name and path, you are prompted for it.

**pem**

Loads a PEM-encoded X.509 private key into the key entry.

**pem** [*keyfilename|url*]

**Syntax Description**

<i>key-filename</i>	The name of the PEM-encoded key file.
<i>url</i>	The location of the file (serial and telnet only).

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not enter the file name and path, you are prompted for it.

---

**Related Commands**

**pem-paste** (Key Configuration Command Set)

## pem-paste

Allows a PEM-encoded X.509 key to be pasted into the configuration manager.

### **pem-paste**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

After the command is entered, you are prompted to paste a key from the cut buffer. You can use a text editor to copy the key from a file. After the key is pasted, you must press **Enter** twice to complete the command.

## Reverse-Proxy Server Configuration Command Set

Use Reverse-Proxy Server Configuration commands to set up and configure reverse-proxy servers. Enter Reverse-Proxy Server Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged mode, the **ssl** command in Configuration mode, and the **reverse-proxy-server** command in SSL Configuration mode. The prompt changes to `<config-ssl-rproxy[servername]>`.

### activate

Activates the current suspended reverse-proxy server if enough information has been configured.

**activate**

---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

All reverse-proxy servers are created as active servers by default.

---

#### Related Commands

**suspend** (Reverse-Proxy Server Configuration Command Set)

### certgroup serverauth

Assigns a certificate group to be used for server certificate authentication.

**certgroup serverauth** *<certgroupname>*  
**no certgroupchain**

---

#### Syntax Description

---

<i>certgroupname</i>	The name of the certificate group.
----------------------	------------------------------------

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to disable server authentication using the certificate group. When using the **no** flag, you need not specify any certificate group name. Only one certificate group can be used.

---

**Related Commands**

**certgroup** (SSL Configuration Command Set)

**show ssl certgroup** (Non-Privileged Command Set)

See also “Certificate Group Configuration Command Set”.

**end**

Exits Reverse-Proxy Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**end**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**exit**

Exits Reverse-Proxy Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Reverse-Proxy Server Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*<command>*]

---

### Syntax Description

*command*

The name of the command.

---

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Reverse-Proxy Server Configuration Commands

## info

Displays current information about the reverse-proxy server being edited or created.

**info**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## localport

Specifies the TCP service port through which non-secure connections are received.

**localport** <*port*|**default**>

<b>Syntax Description</b>	<i>port</i>	The used to transfer non-secure traffic.
	<b>default</b>	Sets the port specification to 80.

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## log-url

Specifies a host for logging of URL requests.

**log-url** <*ipaddr*>

<b>Syntax Description</b>	<i>ipaddr</i>	The IP address of the host for the log.
---------------------------	---------------	---

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## secpolicy

Creates an association between this server and the specified security policy.

**secpolicy** <*polname*|**all**|**default**|**fips**|**noexport56**|**strong**|**weak**>

<b>Syntax Description</b>	<i>polname</i>	The name of the configured security policy.
	<b>all</b>	All pre-loaded security policies.
	<b>default</b>	Default security policy set.

<b>fips</b>	FIPS 104-2-compliant security policy set.
<b>noexport56</b>	Security policy set used to address potential problems in non-US installations using Internet Explorer. While this security policy disables the 56-bit cipher suite, it does not compromise the strength or the integrity of the encryption in any way.
<b>strong</b>	Strong security policy set.
<b>weak</b>	Weak security policy set.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Several default security policies are preloaded into the SSL device. To see a list of all loaded default and user-defined security policies, use the **show ssl secpolicy** command.

### Related Commands

**secpolicy** (SSL Configuration Command Set)

**show ssl secpolicy** (Non-Privileged Command Set)

See the section “Security Policy Configuration Command Set”.

## serverauth enable

Enables server certificate authentication.

**serverauth enable**

**no serverauth enable**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### Related Commands

**certgroup serverauth** (Reverse-Proxy Configuration Command Set)

**serverauth ignore** (Reverse-Proxy Server Configuration Command Set)

## serverauth ignore

Specifies the server authentication errors to ignore.

```
serverauth ignore <all | none|signature-failure|expired-date|
cert-not-yet-valid|invalid-ca|domain-name>
no serverauth ignore< all | none|signature-failure|expired-date|
cert-not-yet-valid|invalid-ca|domain-name>
```

Syntax Description		
	<b>all</b>	Ignore all server authentication errors.
	<b>non</b>	Do not ignore server authentication errors.
	<b>signature-failure</b>	Ignore certificate signature failure errors.
	<b>expired-date</b>	Ignore certificate expiration errors.
	<b>cert-not-yet-valid</b>	Ignore errors caused by using the certificate before it is valid.
	<b>invalid-ca</b>	Ignore errors caused by an unrecognized CA.
	<b>domain-name</b>	Ignore errors due to an invalid domain name.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Any combination of options can be used currently. Use the **no** form of the command to cease ignoring the specific server authentication error.

### Related Commands

**certgroup serverauth** (Reverse-Proxy Server Configuration Command Set)  
**serverauth enable** (Reverse-Proxy Server Configuration Command Set)

## session-cache enable

Enables session caching.

```
session-cache enable
no session-cache enable
```



**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands** **session-cache size** (Reverse-Proxy Server Configuration Mode)  
**session-cache timeout** (Reverse-Proxy Server Configuration Mode)

## session-cache size

Specifies the size of the session cache.

**session-cache size** *<cache size>*

<b>Syntax Description</b>	<i>cache size</i>	The number of cached sessions. The default is 1024. The acceptable range is 1 to 76,800.
---------------------------	-------------------	--

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands** **session-cache enable** (Reverse-Proxy Server Configuration Mode)  
**session-cache timeout** (Reverse-Proxy Server Configuration Mode)

## session-cache timeout

Specifies the session cache length before being timed out.

**session-cache timeout** *<seconds>*

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds before the cache times out.
---------------------------	----------------	---

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

---

**Related Commands**

**session-cache enable** (Reverse-Proxy Server Configuration Mode)  
**session-cache size** (Reverse-Proxy Server Configuration Mode)

**suspend**

Suspends the function of the backend server.

**suspend [now]**

---

**Syntax Description**

---

<b>now</b>	Suspends actions of the backend server immediately.
------------	---

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

This command behaves in three ways:

- If you are creating a new reverse-proxy server and you use the **suspend** command, the server is created in the suspended state. No connections are accepted until the **activate** command is used.
- If you are editing an existing reverse-proxy server and you use the **suspend** command alone, the all open connections on the server are finished, and no new connections are accepted. No connections are accepted until the **activate** command is used.
- If you are editing an existing reverse-proxy server and you use the **suspend now** command, all connections are suspended. When the **end** command is entered, the current reverse-proxy server is removed, and a new suspended reverse-proxy server is created.

---

**Related Commands**

**activate** (Reverse-Proxy Server Configuration Mode)

## Security Policy Configuration Command Set

Use Security Policy Configuration commands to set up and manage security policies. Enter Security Policy Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged Mode, the **ssl** command in Configuration mode, and **secpolicy** command in SSL Configuration mode. The prompt changes to `<config-ssl-secpolicy[secpolicyname]>>`.

### crypto

Creates a customized security policy for the current SSL device.

```
crypto <fips | noexport56 | strong | weak | all | ARC4-MD5 | ARC4-SHA |
DES-CBC3-MD5 | DES-CBC3-SHA | DES-CBC-MD5 |
DES-CBC-SHA | EXP-ARC2-MD5 | EXP-ARC4-MD5 |
EXP-ARC4-SHA | EXP-DES-CBC-SHA |
EXP1024-ARC2-CBC-MD5 | EXP1024-ARC4-MD5 |
EXP1024-ARC4-SHA | EXP1024-DES-CBC-SHA | NULL-MD5 |
NULL-SHA >
no crypto < ARC4-MD5 | ARC4-SHA | DES-CBC3-MD5 |
DES-CBC3-SHA | DES-CBC-MD5 | DES-CBC-SHA |
EXP-ARC2-MD5 | EXP-ARC4-MD5 | EXP-ARC4-SHA |
EXP-DES-CBC-SHA | EXP1024-ARC2-CBC-MD5 |
EXP1024-ARC4-MD5 | EXP1024-ARC4-SHA |
EXP1024-DES-CBC-SHA | NULL-MD5 | NULL-SHA >
```

**Syntax Description** The following table shows the characteristics of each cryptographic algorithm.

Cryptographic Scheme	Encryption	Message Authentication	Key Exchange	Security Policy Assignments
ARC4-MD5	ARC4 <sup>1</sup> (128)	MD5	RSA (1024)	noexport56, strong, default, all
ARC4-SHA	ARC4 <sup>1</sup> (128)	SHA1	RSA (1024)	noexport56, strong, default, all

Cryptographic Scheme	Encryption	Message Authentication	Key Exchange	Security Policy Assignments
DES-CBC3-MD5	3DES (168)	MD5	RSA (1024)	noexport56, strong, all
DES-CBC3-SHA	3DES (168)	SHA1	RSA (1024)	fips, noexport56, strong, all
DES-CBC-MD5	DES (56)	MD5	RSA (1024)	strong, all
DES-CBC-SHA	DES (56)	SHA1	RSA (1024)	fips, strong, all
EXP-ARC2-MD5	ARC2 <sup>2</sup> (40)	MD5	RSA (512)	noexport56, weak, all
EXP-ARC4-MD5	ARC4 <sup>1</sup> (40)	MD5	RSA (512)	noexport56, weak, default, all
EXP-ARC4-SHA	ARC4 <sup>1</sup> (40)	SHA1	RSA (512)	weak, default, all
EXP-DES-CBC-SHA	DES (40)	SHA1	RSA (512)	noexport56, weak, all
EXP1024-ARC2-CBC-MD5	ARC2 <sup>2</sup> (40)	MD5	RSA (1024)	weak, default, all
EXP1024-ARC4-MD5	ARC4 <sup>1</sup> (40)	MD5	RSA (1024)	weak, default, all
EXP1024-ARC4-SHA	ARC4 <sup>1</sup> (40)	SHA1	RSA (1024)	weak, default, all
EXP1024-DES-CBC-SHA	DES (40)	SHA1	RSA (1024)	weak, all
NULL-MD5	None	MD5	None	weak, default, all
NULL-SHA	None	SHA1	None	weak, default, all

<sup>1</sup>ARC4 is compatible with RC4™ RSA Data Security.

<sup>2</sup>ARC2 is compatible with RC2™ RSA Data Security.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

(This command must be entered on one line.) You can identify either individual ciphers or use the **fips, noexport56, strong, weak, default, or all** keywords to specify cipher sets.

The **no** form of this command is used to remove a cipher or set of ciphers. You must specify which algorithm(s) to remove following the **no crypto** command. For example, using the commands **crypto ARC4-MD5** and **crypto ARC4-SHA** loads both schemes into the current user-defined security policy. Additionally, you can alter the preset cryptography schemes specified for the current security policy. If you enter **crypto weak** and **no crypto NULL-MD5** commands, the **NULL-MD5** cryptography scheme is removed from the current security policy.



---

**Note** “ARC4” is compatible with RC4™ RSA Data Security. “ARC2” is compatible with RC2™ RSA Data Security. The “strong” policy includes ARC4-MD5, ARC4-SHA, DES-CBC3-MD5, DES-CBC3-SHA, DES-CBC-MD5, and DES-CBC-SHA. The “weak” policy includes all policies prefixed with “EXP-” “NULL-”. These policies are considered to be export-level policies.

---



---

**Note** In FIPS Mode, only FIPS-approved algorithms (DES-CBC-SHA, DES-CBC3-SHA) are available.

---

**end**

Exits Security Policy Configuration mode, activates all changes, and returns to SSL Configuration mode.

**end**

---

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## exit

Exits Security Policy Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Security Policy Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

---

<i>command</i>	The name of the command.
----------------	--------------------------

---

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Security Policy Configuration Commands

## info

Displays current information about the security policy being edited or created.

### info

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## urlrewrite

Sets or remove a specified URL rewrite rule for the current reverse proxy server.

```
urlrewrite <domainName> [sslport <portid>] [clearport <portid>]
<redirectonly>
no urlrewrite <domainName>
```

#### Syntax Description

<i>domainName</i>	The domain or file identifier as a domain name, IP address, or path and file name.
<b>sslport</b>	A keyword identifying the following <i>portid</i> to be used for SSL traffic.
<i>portid</i>	The TCP service port to be used for SSL traffic.
<b>clearport</b>	A keyword identifying the following <i>portid</i> to be used for clear text traffic.
<i>portid</i>	The TCP service port to be used for clear text traffic.
<b>redirectonly</b>	A keyword is used to indicate that only the “Location;” field in the HTTP 30x redirect header should be rewritten. This solves a common problem with Web servers using insecure HTTP 30x redirects.

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

An \* (asterisk) wild card character can be used to specify more than one server in a single domain, e.g., “\*.company.com”. Up to 32 URL rewrite rules can be configured. Use the **no** form of the command to clear the specified rule. If more

than one rule has been configured, you must specify the domain name of the rule to delete. URL rewrite information can be displayed by using the command **show ssl server**.

---

**Related Commands**    **show ssl server** (Non-Privileged Command Set)



## Server Configuration Command Set

Use Server Configuration commands to set up and configure logical secure servers. Enter Server Configuration mode by using the **enable** command in Non-Privileged mode, the **configure** command in Privileged mode, the **ssl** command in Configuration mode, and the **server** command in SSL Configuration mode. The prompt changes to `<config-ssl-server[servername]>>`.

### activate

Activates the current logical secure server if enough information has been configured.

**activate**

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

#### Related Commands

**suspend** (Server Configuration Command Set)

### cert

Sets the specified certificate for use by the server.

**cert** *<certname | default | default-1024 | default 512>*

#### Syntax Description

<i>certname</i>	The name of the certificate.
<b>default</b>	The pre-loaded default certificate.
<b>default-1024</b>	The pre-loaded 1024-bit default certificate.
<b>default-512</b>	The pre-loaded 512-bit default certificate.

#### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Only one certificate is allowed per server. If you enter this command with a different certificate, that reference replaces the earlier one.

---

### Related Commands

**certificate** (SSL Configuration Command Set)

**show ssl cert** (Non-Privileged Command Set)

See also “Certificate Configuration Command Set”.

## certgroup chain

Enables the specified certificate group to be used as a certificate chain. The **no** form of the command is used to disable certificate chaining.

**certgroup chain** *certgroupname*

**no certgroupchain**

---

### Syntax Description

<i>certgroupname</i>	The name of the certificate group.
----------------------	------------------------------------

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to remove a certificate group association. When using the **no** flag, you need not specify any certificate group name. Only one certificate chain is allowed.

---

### Related Commands

**certgroup** (SSL Configuration Command Set)

**show ssl certgroup** (Non-Privileged Command Set)

See also “Certificate Group Configuration Command Set”.

## certgroup clientauth

Assigns a certificate group to be used as a certificate trust list for client certificate authentication.

**certgroup clientauth** <certgroupname>  
**no clientauth**

---

**Syntax Description**

---

*certgroupname*                      The name of the certificate group.

---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The **no** form of the command is used to disable client authentication using the certificate group. When using the **no** flag, you need not specify any certificate group name. Only one certificate chain can be used.

---

**Related Commands**

**clientauth enable** (Server Configuration Command Set)  
**clientauth error** (Server Configuration Command Set)  
**clientauth verifydepth** (Server Configuration Command Set)

## clientauth enable

Enables client certificate authentication.

**clientauth enable**  
**no clientauth enable**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Use the **no** form of the command to disable client certificate authentication.

---

**Related Commands**

**certgroup enable** (Server Configuration Command Set)  
**clientauth error** (Server Configuration Command Set)  
**clientauth verifydepth** (Server Configuration Command Set)

## clientauth error

Specifies the client certificate authentication errors to ignore.

```
clientauth error <cert-not-provided|cert-not-yet-valid|cert-has-expired|
cert-revoked|cert-has-invalid-ca|cert-has-signature-failure|cert-oth-
er-error|all> <fail|failhtml|ignore|redirect <url>>
no clientauth error <cert-not-provided|
cert-not-yet-valid|cert-has-expired|cert-revoked|
cert-has-invalid-ca|cert-has-signature-failure|cert-other-error|all >
```

### Syntax Description

<b>cert-not-provided</b>	Certificate was not provided for authentication.
<b>cert-not-yet-valid</b>	The certificate is not valid yet.
<b>cert-has-expired</b>	The certificate has expired.
<b>cert-revoked</b>	The certificate has been revoked.
<b>cert-has-invalid-ca</b>	The certificate has an invalid CA.
<b>cert-has-signature-failure</b>	The signature on the certificate failed.
<b>cert-other-error</b>	Any other certificate authentication error.
<b>all</b>	All certificate authentication errors, including those listed above.
<b>fail</b>	The client is disconnected abruptly.
<b>failhtml</b>	The SSL handshake is continued and the client is sent a static HTML error page listing the reason for the error. Then the SSL session is disconnected.
<b>ignore</b>	The server silently ignores the authentication error and continues the SSL connection.
<b>redirect</b>	The SSL handshake is continued and the client is redirected to another HTML page specified by the <i>url</i> argument. The SSL session is disconnected.
<i>url</i>	The location of the error page for redirection.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Any combination of options can be used currently. Use the **no** form of the command to cease ignoring the specific client authentication error.

**Related Commands**

**certgroup clientauth** (Server Configuration Command Set)

**clientauth enable** (Server Configuration Command Set)

**clientauth verifydepth** (Server Configuration Command Set)

**clientauth verifydepth**

Specifies the level of certificate within the certificate group to use when verifying client certificates.

**clientauth verifydepth** <depth>

**Syntax Description**

<i>depth</i>	The number of certificates within the certificate group to use for authentication.
--------------	--

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**certgroup clientauth** (Server Configuration Command Set)

**clientauth enable** (Server Configuration Command Set)

**clientauth error** (Server Configuration Command Set)

**end**

Exits Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**end**

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## ephemeral error

Specifies device behavior when an error is caused by a client attempting to attach to a server that does not have ephemeral RSA enabled.

**ephemeral error** <fail|failhtml|redirect <url>>

<b>Syntax Description</b>	<b>fail</b>	The client is disconnected abruptly.
	<b>failhtml</b>	The SSL handshake is continued and the client is sent a static HTML error page listing the reason for the error. Then the SSL session is disconnected. (Default)
	<b>redirect</b>	The SSL handshake is continued and the client is redirected to another HTML page specified by the <i>url</i> argument. The SSL session is disconnected.
	<i>url</i>	The location of the error page for redirection.

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The default behavior is **failhtml**.

## ephrsa

When an export browser version connects to a server using 1024-bit keys, this allows the RSA key exchange (the SSL handshake) to be negotiated using a dynamically created 512-bit key. Using ephemeral RSA ensures the device complies with United States commerce laws.

**ephrsa**  
**no ephrsa**

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The default is no ephemeral RSA. Use the **no** form of the command to disable ephemeral RSA.

## exit

Exits Server Configuration mode, activates all changes, and returns to SSL Configuration mode.

**exit**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## finished

Leaves Server Configuration Mode and returns to Top Level mode.

**finished**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## help

Displays help information for the specified command.

**help** [*command*]

---

### Syntax Description

---

<i>command</i>	The name of the command.
----------------	--------------------------

---

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

If you do not specify a command, help information is displayed for all Server Configuration Commands

## httpheader

Specifies the header information to pass to backend HTTP servers.

```

httpheader <session|server-cert|client-cert|pre-filter|prefix
  <prefixString>>
no httpheader <session|server-cert|client-cert|pre-filter|prefix>

```

---

### Syntax Description

<b>session</b>	Adds SSL session information to the HTTP stream.
<b>server-cert</b>	Adds the server certificate to the HTTP stream.
<b>client-cert</b>	Adds the client certificate to the HTTP stream.
<b>pre-filter</b>	Pre-filters the client header.
<b>prefix</b>	Allows a prefix string to be added to the HTTP stream.
<i>prefixString</i>	The string to use as a header prefix.

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

(This command must be entered on one line.) Any combination of options can be used currently. Use the **no** form of the command to cease using the specific option.

### info

Displays current information about the logical secure server being edited or created.

**info**

---

### Usage Guidelines

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

### ip address

Sets the specified IP address for the logical secure server. Using the **no** form of the command clears the IP address for the logical secure server.

```

ip address <ipaddr> [netmask <mask>]
no ip address

```



<b>Syntax Description</b>	<i>ipaddr</i>	The IP address to assign to the secure server.
	<b>netmask</b> < <i>mask</i> >	The netmask valid for the IP address.

**Usage Guidelines**      Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

## key

Sets the specified key for use by the server.

**key** <*keyname* | **default** | **default-1024** | **default 512**>

<b>Syntax Description</b>	<i>keyname</i>	The name of the key.
	<b>default</b>	The pre-loaded default key.
	<b>default-1024</b>	The pre-loaded 1024-bit default key.
	<b>default-512</b>	The pre-loaded 512-bit default key.

**Usage Guidelines**      Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Only one key is allowed per server. If you enter this command with a different key, that reference replaces the earlier one.

**Related Commands**      **key**(SSL Configuration Command Set)  
**show ssl key** (Non-Privileged Command Set)

See also “Key Configuration Command Set”.

## localport

Specifies the port on which the secure server receives SSL traffic. The SSL traffic is decrypted and sent to the real server using the TCP service port previously specified with the **remotepoint** command.

**localport** <port|default>

<b>Syntax Description</b>	<i>port</i>	The TCP service port through which SSL traffic is received by the current secure logical server.
	<b>default</b>	Returns the setting to the default of 443.

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands** **remoteport** (Server Configuration Command Set)  
**sslport** (Server Configuration Command Set)

**log-url**

Specifies a host for logging of URL requests.

**log-url** <ipaddr>

<b>Syntax Description</b>	<i>ipaddr</i>	The IP address of the host for the log.
---------------------------	---------------	---

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**remoteport**

Specifies the TCP service port through which non-secure connections is sent.

**remoteport** <port|default>

<b>Syntax Description</b>	<i>port</i>	The non-secure port used to send clear text traffic to the server.
	<b>default</b>	Sets the non-secure port specification to 80.

**Caution**


---

Traffic sent on this TCP service port is not secured by SSL during transmission to the server. It must be secured by another means.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**

**localport** (Server Configuration Command Set)  
**sslport** (Server Configuration Command Set)

**secpolicy**

Creates an association between this server and the specified security policy.

**secpolicy** <polname|all|default|fips|noexport56|strong|weak>

**Syntax Description**

<i>polname</i>	The name of the configured security policy.
<b>all</b>	All pre-loaded security policies.
<b>default</b>	Default security policy set.
<b>fips</b>	FIPS 104-2-compliant security policy set.
<b>noexport56</b>	Security policy set used to address potential problems in non-US installations using Internet Explorer. While this security policy disables the 56-bit cipher suite, it does not compromise the strength or the integrity of the encryption in any way.
<b>strong</b>	Strong security policy set.
<b>weak</b>	Weak security policy set.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

Several default security policies are preloaded into the SSL device. To see a list of all loaded default and user-defined security policies, use the **show ssl secpolicy** command.

**Related Commands**    **secpolicy** (SSL Configuration Command Set)  
**show ssl secpolicy** (Non-Privileged Command Set)

See the section “Security Policy Configuration Command Set”.

## session-cache enable

Enables session caching.

**session-cache enable**  
**no session-cache enable**

**Usage Guidelines**    Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*  
 Use the **no** form of the command to disable session caching.

**Related Commands**    **session-cache size** (Server Configuration Mode)  
**session-cache timeout** (Server Configuration Mode)

## session-cache size

Specifies the size of the session cache.

**session-cache size** *<cache size>*

<b>Syntax Description</b>	<i>cache size</i>	The number of sessions. The default is 1024. The acceptable range is 1 to 76,800.
---------------------------	-------------------	---

**Usage Guidelines**    Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands**    **session-cache enable** (Server Configuration Mode)  
**session-cache timeout** (Server Configuration Mode)

## session-cache timeout

Specifies the session cache length before being timed out.

**session-cache timeout** <*seconds*>

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds before the cache times out.
---------------------------	----------------	---

**Usage Guidelines** Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

**Related Commands** **session-cache enable** (Server Configuration Mode)  
**session-cache size** (Server Configuration Mode)

## sharedcipher error

Specifies device behavior when an error caused by no cipher agreement is encountered.

**sharedcipher error** <**fail|failhtml|redirect** <*url*>>

<b>Syntax Description</b>	<b>fail</b>	The client is disconnected abruptly.
	<b>failhtml</b>	The SSL handshake is continued and the client is sent a static HTML error page listing the reason for the error. Then the SSL session is disconnected. (Default)
	<b>redirect</b>	The SSL handshake is continued and the client is redirected to another HTML page specified by the <i>url</i> argument. The SSL session is disconnected.
	<i>url</i>	The location of the error page for redirection.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

The default behavior is **failhtml**.

## sslport

Specifies the port on which the logical secure server receives SSL traffic. The SSL traffic is decrypted and sent to the physical server using the TCP service port previously specified with the **remoteport** command.

**sslport** <port|default>

---

**Syntax Description**

<i>port</i>	The TCP service port through which SSL traffic is received by the current secure logical server.
<b>default</b>	Returns the setting to the default of 443.

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*



**Note** This command has the same effects as the **localport** command and is included only for backwards compatibility.

---

**Related Commands**

**localport** (Server Configuration Command Set)  
**remoteport** (Server Configuration Command Set)

## suspend

Suspends the function of the server.

**suspend** [now]

---

**Syntax Description**

<b>now</b>	Suspends actions of the server immediately.
------------	---

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

This command behaves in three ways:

- If you are creating a new server and you use the **suspend** command, the server is created in the suspended state. No connections are accepted until the **activate** command is used.
- If you are editing an existing server and you use the **suspend** command alone, the all open connections on the server are finished, and no new connections are accepted. No connections are accepted until the **activate** command is used.
- If you are editing an existing server and you use the **suspend now** command, all connections are suspended. When the **end** command is entered, the current server is removed, and a new suspended server is created.

---

**Related Commands**

**activate** (Server Configuration Mode)

**transparent**

Enables to servers to function as a transparent proxy (default). The **no** form of the command is used to disable this behavior.

**transparent**  
**no transparent**

---

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

When transparent proxy behavior is disabled, the device accepts connections on the IP address of the Secure Content Accelerator rather than on the server address.

**urlrewrite**

Sets or remove a specified URL rewrite rule for the current secure server.

**urlrewrite** *<domainName>* [**sslport** *<portid>*] [**clearport** *<portid>*]  
**<redirectonly>**  
**no urlrewrite** *<domainName>*

<b>Syntax Description</b>	<i>domainName</i>	The domain or file identifier as a domain name, IP address, or path and file name.
	<b>sslport</b>	A keyword identifying the following <i>portid</i> to be used for SSL traffic.
	<i>portid</i>	The TCP service port to be used for SSL traffic.
	<b>clearport</b>	A keyword identifying the following <i>portid</i> to be used for clear text traffic.
	<i>portid</i>	The TCP service port to be used for clear text traffic.
	<b>redirectonly</b>	A keyword is used to indicate that only the “Location;” field in the HTTP 30x redirect header should be rewritten. This solves a common problem with Web servers using insecure HTTP 30x redirects.

**Usage Guidelines**

Availability: *Remote, Serial, Telnet; FIPS Mode (serial only)*

An \* (asterisk) wild card character can be used to specify more than one server in a single domain, e.g., “\*.company.com”. Up to 32 URL rewrite rules can be configured. Use the **no** form of the command to clear the specified rule. If more than one rule has been configured, you must specify the domain name of the rule to delete. URL rewrite information can be displayed by using the command **show ssl server**.

**Related Commands**

**show ssl server** (Non-Privileged Command Set)





# Troubleshooting

---

This appendix provides general troubleshooting information for the Secure Content Accelerator. This appendix contains the section “Troubleshooting the Hardware”

# Troubleshooting the Hardware

Table D-1 lists some problems that may occur with the Secure Content Accelerator and recommended actions to take. If you can connect to the device, use the **show diagnostic-report** command to create a file for review. Following the table and three flowcharts you can use to help solve device problems.

*Table D-1 Troubleshooting the Hardware*

Possible Problem	Recommended Action
Link LED is off.	Ensure the Secure Content Accelerator is powered on. Ensure the cable connections are secure. Ensure you are using the correct type of cable (straight-through to connect to a switch or hub; crossover to connect to NIC. Ensure cables are properly wired.
One Power LED is unlit.	Ensure the Secure Content Accelerator has power. Check the associated power switch, power cord, and power source.
The Secure Content Accelerator seems to have locked up.	Reboot the Secure Content Accelerator either by pressing the reset switch or using the <b>reload</b> command in the configuration manager. If the problem continues, press and hold the reset switch for two seconds. In either case, the configuration stored in the flash memory is used when the Secure Content Accelerator reboots.
The configuration manager cannot find the appliance on the network (hardware).	Make sure the cable segment is compliant with 100Base-TX recommendations. The length should not exceed 100 meters (328 feet). Make sure the speed and duplex settings on the SSL device and other networking hardware agree. Using the configuration manager, enter the <b>show interface</b> command to display the settings for the appliance Ethernet interfaces. Make sure you have a valid networking topology.

Table D-1 Troubleshooting the Hardware (continued)

Possible Problem	Recommended Action
<p>The configuration manager cannot find the appliance on the network (software).</p>	<p>Make sure the computer you are using to configure the device or module is on the same subnet and VLAN (if applicable) as the appliance. Once the appliance is configured with an IP address, you can attach it from any point in the network by using the <b>attach ip</b> command. If you are running the configuration manager and install a new device, enter the <b>discover</b> command to find new devices in the same broadcast domain.</p> <p>Make sure remote management and/or telnet management are enabled, as appropriate. Use the <b>show device</b> command using a serial management session to verify management access. If remote management is disabled, enter Configuration mode and use the <b>remote-management enable</b> command. If telnet management is disabled, use the <b>telnet enable</b> command. Also verify the TCP port specified for management sessions. If you have changed the remote management port from the default, you must use the <b>discover port</b> command, where <i>port</i> is the TCP port.</p> <p>The device might be operating in FIPS Mode. Remote management is unavailable in FIPS Mode. Use a serial management session to connect to the device.</p>

Table D-1 Troubleshooting the Hardware (continued)

Possible Problem	Recommended Action
The GUI cannot connect to the device.	<p>Use any CLI configuration manager method to ensure that web management is enabled. Attach to the appliance, if necessary, <b>show device</b> command. If web management is not enabled, use the <b>web-mgmt enable</b> command in Configuration mode to enable it. If you are attempting to connect to appliance from the client side (“Network” port) in two-port mode, you must first set up a secure server. See “Configuring for Client-Side Access” in Chapter 6 for more instructions. If you have changed the IP address during a GUI management session, automatic redirection may not occur in certain situations, such as when changing to a different subnet. If the connection is not redirected, manually connect to the device as before. If you still are unable to connect, use the serial configuration manager to check the appliance configuration and try again.</p> <p>The device might be operating in FIPS Mode. Web management is unavailable in FIPS Mode. Use a serial management session to connect to the device.</p>
The serial management CLI prompt contains “[FIPS]”.	The device is operating in FIPS Mode. If you wish to return the device to normal operation, use the Privileged Mode command <b>no fips enable</b> . See “Returning to Normal Operation” in Chapter 6 for more information.
Only the “fips” security policy is available when configuring servers.	The device is operating in FIPS Mode. Only security policies containing FIPS 140-2-compliant algorithms are available in FIPS Mode.
One or more servers is unavailable for configuration.	The device might be operating in FIPS Mode. Only servers configured with FIPS 140-2-compliant algorithms are available.

Figure D-1 Troubleshooting Flowchart 1

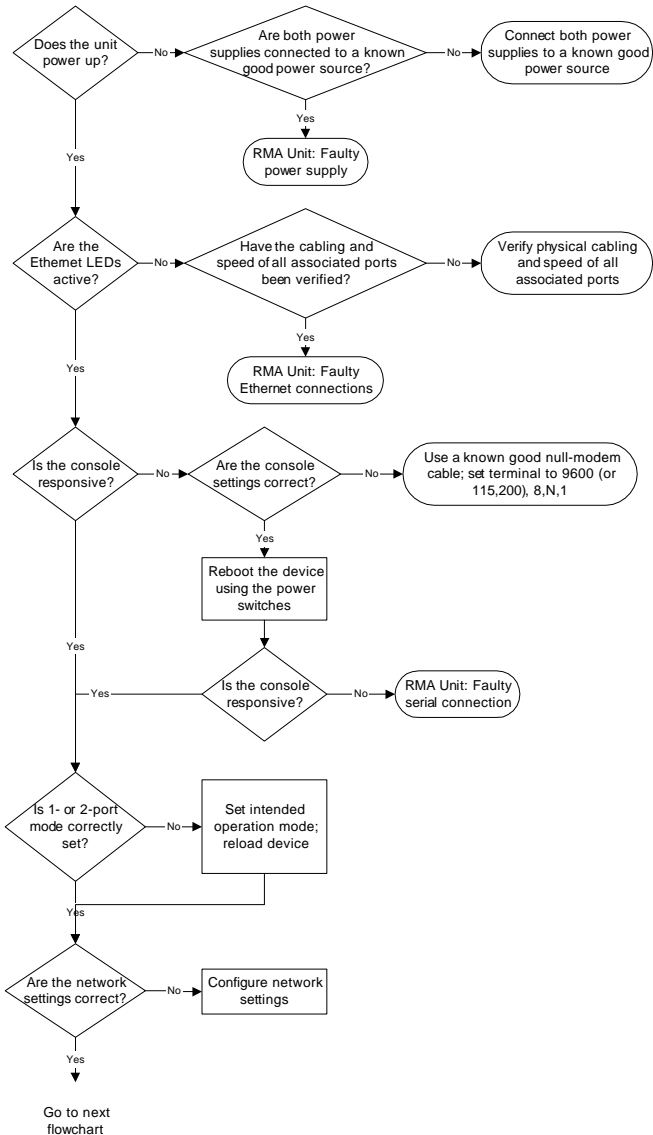


Figure D-2 Troubleshooting Flowchart 2

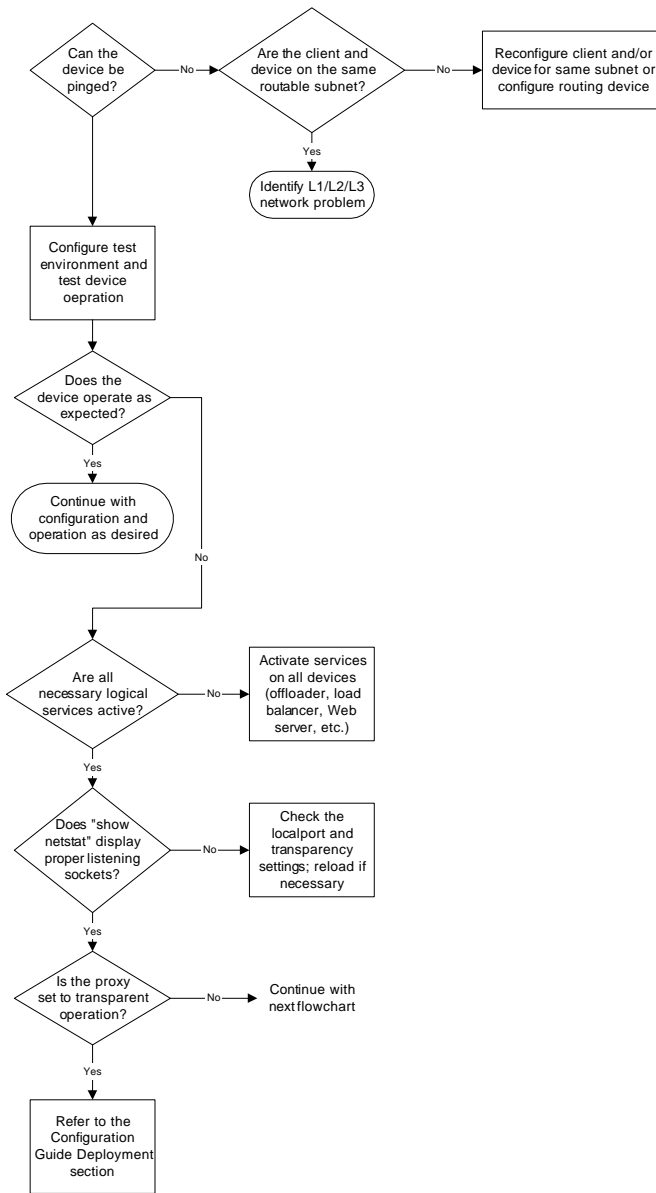
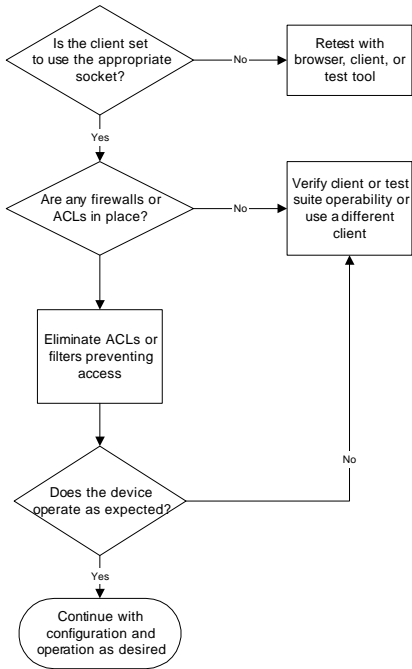


Figure D-3 Troubleshooting Flowchart 3









## SSL Introduction

---

This chapter presents a short introduction to basic SSL components and a description of how the components are used in configuring the Secure Content Accelerator. Instructions for generating keys and certificates using the CLI are included in Chapter 4. Instructions for using the GUI are in Chapter 5.

This chapter contains the following sections:

- Introduction to SSL
- Port Blocking Mechanism
- Before You Begin
- Using Existing Keys and Certificates
- Configuration Security
- Cisco SSL Configuration Components
- Cisco Secure Content Accelerator Management

# Introduction to SSL

Secure Sockets Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys.

Certificates are similar to digital ID cards. They prove the identity of the server to clients. Certificates are issued by Certificate Authorities (CAs) such as VeriSign® or Thawte. Each certificate includes the name of the authority that issued it, the name of the entity to which the certificate was issued, the entity's public key, and time stamps that indicate the certificate's expiration date.

Public and private keys are the ciphers used to encrypt and decrypt information. While the public key is shared quite freely, the private key is never given out. Each public-private key pair works together: data encrypted with the public key can only be decrypted with the private key.

You can configure the Cisco Secure Content Accelerator using either the GUI or CLI, or through the QuickStart wizard (available through both the CLI and GUI). The CLI is available through remote, telnet, or serial connections.

## Port Blocking Mechanism

During configuration you must specify the SSL and clear text (decrypted) TCP service ports. Cisco Secure Content Accelerator devices monitor the SSL TCP service port(s) you specify, perform SSL decoding of packets on those ports, then send the packets to the server via a user-defined TCP clear text service port. All other network traffic is passed through the appliance transparently.

The clear text TCP service port used for data transfer between the SSL appliance and the Web server cannot be used for any other data. The SSL appliance blocks access to the clear text port, protecting your secure data from direct clear text access.

One result of this port blocking strategy is that you cannot use the same clear text TCP service port between the SSL appliance and the server for both non-secure (http:) and decrypted secure data (https:) transfer. Network port traffic received on the clear text TCP service port is dropped. See the figures below.

Figure E-1 Port Blocking

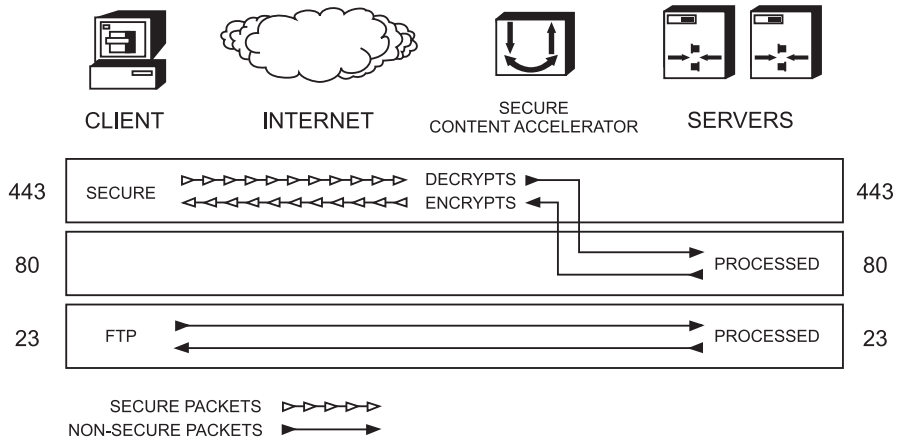
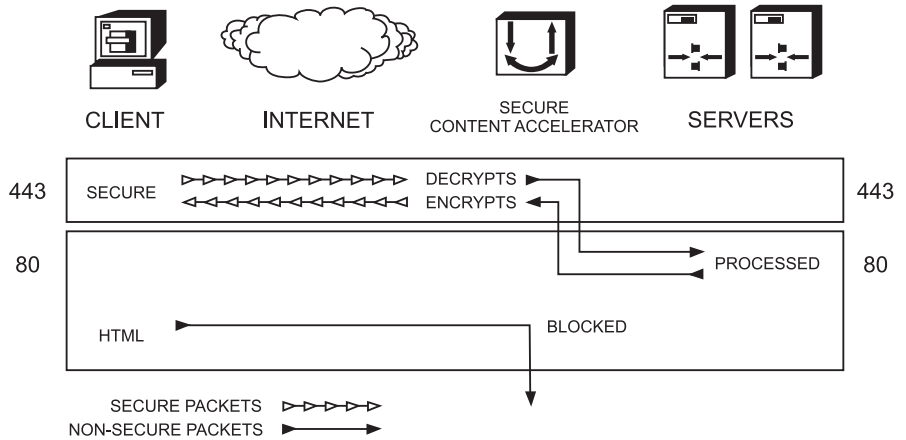


Figure E-2 Port Blocking with Dropped Traffic



For example, if the server is used for both secure and non-secure services, you cannot use TCP service port 80 for both basic HTTP connections and for transfer of decrypted secure data between the devices and the server. Below are some alternatives for this scenario.

- Use 443 (generally used for SSL transactions) as the SSL TCP service port and 443 as the clear text port. Configure the server to not use SSL and to monitor port 443. TCP service port 80 requests are serviced normally.
- Use 443 as the SSL TCP service port and 81 (or another unused port) for the clear text port. Configure the server to monitor port 81. TCP service port 80 requests are serviced normally.

All data sent on any other port is passed through transparently in both directions.

## Before You Begin

Before configuring the SSL appliance you must have a certificate and keys for the server. You can use the files you received from the Certificate Authority, copy the keys and certificate from an existing secure server, use default keys and certificates preloaded in the device, or generate your own keys and certificates.

Additionally, be aware that you must make several changes to your Web pages. The nature of the changes depends upon whether you are securing a previously unsecured site, or adding the SSL appliance to an already secure server installation. These changes are described in section “Web Site Changes” in Appendix B.

## Using Existing Keys and Certificates

If you already have a secure server, you can transfer the keys and certificate to the Secure Content Accelerator. Follow the instructions below, or refer to the Web server software documentation for detailed information.



### Note

---

Key and certificate file names cannot contain spaces and must be compatible with the server operating system. When prompted either to name a key or certificate file or check the name of a key or certificate file, please ensure the names follow these conventions.

---

## Apache mod\_SSL

The key and certificate locations are listed in the **\$APACHEROOT/conf/httpd.conf** file. The default key is **\$APACHEROOT/conf/ssl.key/\*.key**. The default certificate is **\$APACHEROOT/conf/ssl.crt/\*.crt**. Note the name and location of these elements.

## ApacheSSL

The key and certificate locations are listed in the **\$APACHESSLROOT/conf/httpd.conf** file. The default key is **\$APACHEROOT/certs/\*.key**. The default certificate is **\$APACHEROOT/certs/\*.crt**. Note the name and location of these elements.

## Stronghold

The key and certificate locations are listed in the **\$STRONGHOLDROOT/conf/httpd.conf** file. The default key is **\$STRONGHOLDROOT/ssl/private/\*.key**. The default certificate is **\$STRONGHOLDROOT/ssl/\*.cert**. Note the name and location of these elements.

## IIS 4 on Windows NT

The certificate file is in the directory specified when the certificate was downloaded.

1. Double-click the certificate file to open the viewer.
2. Click the **Details** tab.
3. Click **Copy to file**. The Certificate Manager Export Wizard opens. Click **Next**.
4. Select the **DER-encoded binary X.509** radio button. Click **Next**.
5. Specify a file name and location. Click **Next**.
6. Click **Finish**.

7. Click **OK** when you see the successful completion notice.
8. Exit the Certificate Manager Export Wizard.
9. Close the certificate viewer.

The keys are located within the Key Ring—the key manager program. Follow these instructions to export a key.

1. Click the **Start** button, point to **Programs>Windows NT 4.0 Option Pack>Microsoft Internet Information Server**, and click **Internet Service Manager**. The Microsoft Management Console opens.
2. Navigate to the Web site using the object list.
3. Right-click the Web site object and click **Properties** in the shortcut menu.
4. Click the **Directory Security** tab.
5. Click **Edit** in the **Secure Communication** panel.
6. Click **Key Manager**.
7. Click the key to export.
8. On the **Key** menu, point to **Export Key**, and click **Backup File**.
9. Read the security warning and click **OK**.
10. Select a file location and enter a file name.
11. Click **Save**.
12. Exit the Internet Service Manager.

## IIS 5 on Windows 2000

Follow these steps to export a certificate and key.

1. Click the **Start** button, point to **Programs>Administrative Tools**, and click **Internet Service Manager**. Alternatively, open the **Internet Service Manager** in the **Administrative Tools** folder in the **Control Panel**.
2. Right-click the Web site object and click **Properties** in the shortcut menu.
3. Click the **Directory Security** tab.
4. Click **View Certificate** in the **Secure Communications** panel. The Certificate Viewer appears.
5. Click the **Details** tab.

6. Click **Copy to File**. The Certificate Export Wizard appears.
7. Click **Next**. The Export Private Key screen appears.
8. Select the **Yes, export the private key** option. Click **Next**. The **Export File Format** panel appears.
9. Select the **Personal Information Exchange—PKCS#12 (pfx)** option and any optional choices desired. Click **Next**. The **Password** panel appears.
10. Type the password in the **Password** and **Confirm Password** text boxes. Click **Next**. The **File to Export** panel appears.
11. Type the path and file name in the **File name** text box or click **Browse** to select a location manually. Click **Next**.
12. The **Completing the Certificate Export Wizard** panel appears. Click **Finish**.

**Note**

---

The key and certificate file exported from IIS 5 are in PKCS#12 format. Use the **import pkcs12** command in the configuration manager to load a key and certificate in this format.

---

## Configuration Security

Cisco Secure Content Accelerator devices allow easy, flexible configuration without compromising the security of your network or their own configuration.

## Passwords

Cisco Secure Content Accelerator devices use two levels of password protection: access- and enable-level. *Access-level passwords* control who can attach the remote configuration manager or access the device via telnet and serial connections. *Enable-level passwords* control who can view the same data available with access-level passwords as well as view sensitive data and configure the device.

SSL devices are shipped without passwords. Setting passwords is important because the device can be administered over a network. For more information about passwords, see the commands **password access** and **password enable** in Appendix C.

## Access Lists

Access lists control which computers can attach to a specific device. No access lists exist when you first install the Secure Content Accelerator. You can restrict the computers allowed to manage the appliance by adding their IP addresses to one or more access lists for each device. For more information about configuring access lists, see the commands **show access-list**, **access-list**, **snmp access-list**, **remote-management access-list**, **telnet access-list**, and **web-mgmt access-list** in Appendix C.

## Encrypted Management Sessions

To further protect the configuration security, you can specify that remote (non-serial and non-telnet) configuration sessions be encrypted using AES, DES, or ARC4. See **remote-management encryption** in Appendix C.

## Factory Default Reset Password

If you have forgotten your access or enable password, you can use a factory-set password during a serial configuration session. When prompted for a password, enter *FailSafe* (case-sensitive). You are asked to confirm the action. The appliance reboots (reloads) with factory default settings.



### Caution

---

All configuration is lost when using the factory default reset password.

---



# Cisco SSL Configuration Components

When you configure an appliance to perform SSL offloading you are actually setting up one or more logical secure servers whose SSL-related configurations reside in the appliance. Each logical secure server has several attributes:

- A unique IP address and TCP port for the real server providing content
- An associated key specifying the public/private key pair to use
- A single certificate or certificate group to use
- A security policy specifying the cryptographic scheme(s) to use

## Real Server IP Addresses

Each SSL server is associated with a specific IP address and TCP port. The address and TCP port are unique and may not be used for more than one SSL server on a single SSL device.

## Keys

A single key can be used with each an individual SSL server. You can load multiple keys into the device; however, only one can be used with each SSL server. Keys can be imported from DER- and PEM-encoded X509-format key files, IIS4 backup key-format (NET-IIS), and PKCS#12 files.

## Certificates

A certificate is loaded into the device to be used as either a single certificate or part of a certificate group. Only one certificate or certificate group can be used with each server. Certificates can be imported from DER- and PEM-encoded X.509 files, IIS4 backup format (NET-IIS), PKCS#12 files, and PCKS#7 certificate groups.

## Step-Up Certificates and Server-Gated Cryptography

Cisco Secure Content Accelerator devices support both Netscape International Step-Up Certificates and Microsoft Server-Gated Cryptography. No special configuration is needed for the device to function properly with these certificates. Load the certificate normally.

**Note**

---

You must specify that your certificate will work with both Microsoft and Netscape browsers when requesting it from the CA. Otherwise, the server cannot support both browsers.

---

## Chained Certificates

Chained certificates are used in certain circumstances such as when a known, trusted CA (such as Thawte or VeriSign) provides a certificate to attest that certificates created by an intermediary CA can be trusted. For example, a company can create its own certificates for internal use only; however, clients do not accept the certificates because they were not created by a known CA. When private certificates are chained with the trusted CA certificate, clients accept them during SSL negotiations.

The certificate created locally is loaded into the device as a regular certificate; the locally created public/private key pair is loaded into the device as a key. The intermediary CA certificate signed by a trusted CA and any other intermediary certificates are loaded as individual certificate objects that are combined into a *certificate group*. An example of configuring a chained certificate via the configuration manager is presented in Chapter 5. See Chapter 6 for information about creating and enabling chained certificates using the GUI.

## Security Policies

Cisco Secure Content Accelerator can process a wide range of single and composite cryptography schemes. The following table shows a comparison of the individual schemes. If you configure the device to use the weak security policy, all schemes marked as “weak” are used. If you use the strong security policy, all schemes marked as “strong” are used. The “default” security policy uses the encryption and message authentication methods commonly available. The “all” security policy incorporates all listed combinations.

**Table E-1 Secure Content Accelerator Cryptographic Algorithms**

Cryptographic Scheme	Encryption	Message Authentication	Key Exchange	Security Policy Assignments
ARC4-MD5	ARC4 <sup>1</sup> (128)	MD5	RSA (1024)	strong, default, all
ARC4-SHA	ARC4 <sup>1</sup> (128)	SHA1	RSA (1024)	strong, default, all
DES-CBC3-MD5	3DES (168)	MD5	RSA (1024)	strong, all
DES-CBC3-SHA	3DES (168)	SHA1	RSA (1024)	strong, fips, all
DES-CBC-MD5	DES (56)	MD5	RSA (1024)	strong, all
DES-CBC-SHA	DES (56)	SHA1	RSA (1024)	strong, fips, all
EXP-ARC2-MD5	ARC2 <sup>2</sup> (40)	MD5	RSA (512)	weak, all
EXP-ARC4-MD5	ARC4 <sup>1</sup> (40)	MD5	RSA (512)	weak, default, all
EXP-ARC4-SHA	ARC4 <sup>1</sup> (40)	SHA1	RSA (512)	weak, default, all
EXP-DES-CBC-SHA	DES (40)	SHA1	RSA (512)	weak, all
EXP1024-ARC2-CBC-MD5	ARC2 <sup>2</sup> (40)	MD5	RSA (1024)	weak, default, all
EXP1024-ARC4-MD5	ARC4 <sup>1</sup> (40)	MD5	RSA (1024)	weak, default, all
EXP1024-ARC4-SHA	ARC4 <sup>1</sup> (40)	SHA1	RSA (1024)	weak, default, all
EXP1024-DES-CBC-SHA	DES (40)	SHA1	RSA (1024)	weak, all
NULL-MD5	None	MD5	None	weak, default, all
NULL-SHA	None	SHA1	None	weak, default, all

<sup>1</sup>ARC4 is compatible with RC4™ RSA Data Security.<sup>2</sup>ARC2 is compatible with RC2™ RSA Data Security.

# Cisco Secure Content Accelerator Management

You can configure the Cisco Secure Content Accelerator using one of four methods, three of which use the CLI configuration manager.

- Serial connection, configuration manager
  - An IP address need not have been assigned for appliance management.
  - A device can be set to single-port mode via serial connection.
  - A device must be managed while physically connected via a serial cable.
  - The FailSafe password can be used as a factory reset.
- Telnet connection, configuration manager
  - An IP address must have been assigned to the appliance.
  - A device cannot be set to single-port mode via telnet.
  - Only one device can be managed at a time.
- Remote network connection, configuration manager application
  - An IP address need not have been assigned for appliance management.
  - A device cannot be set to single-port mode via the remote connection.
  - Multiple devices can be attached.
- Remote network connection, GUI
  - In IP address must have been assigned to the appliance for management.
  - A device cannot be set to single-port mode via the GUI.
  - Only one device can be managed at a single time.

Additionally, the behaviors of some commands vary depending upon the management method. The configuration information for the commands **ip name-server**, **rdate-server**, and **ip domain-name** can be set remotely, but the configuration information is used only through a serial or telnet connection. The results of the **ping** and **traceroute** commands also are dependent upon the management method. When used with the remote management application, these commands are executed and results returned based upon the configuring computer's hardware information. When used with serial or telnet management, the results are based upon the SSL appliance's hardware information.

Serial and telnet management commands can use symbolic hostnames in URL identifiers if the **ip domain-name** has been set.

File name formats differ depending on the management method. When using remote management, you can specify the file name as it appears in the configuring computer's file system. A path must be included, if necessary. When using serial or telnet management, the file name must be entered in any of the following formats:

```
[<http:// | ftp:// | https:// | tftp:// >] URL
```

In situations where a file is written, anonymous write access must be configured on the system with these caveats:

- http:—The server must be configured to accept PUT commands
- https:—The server must be configured to accept PUT commands
- ftp:—If anonymous write access is not allowed, use this format:  
**ftp://username:password@host/directory/filename**
- tftp:—Use this format:  
**tftp://host/filename**  
where the hostname may be either a URL or IP address

Additionally, we provide a guided QuickStart wizard configuration method, available from both the configuration manager and GUI. To use this method for configuration, see Chapter 3. Brief instructions are also included for initiating a management session using the configuration manager.

For instructions on using any of the CLI configuration managers, see Chapter 4; for instructions on using the GUI, see Chapter 5. To use the Secure Content Accelerator in FIPS-compliant operation mode, see Chapter 6.





## Regulatory Information

---

This appendix lists the regulatory agencies that have approved the Secure Content Accelerator.

This appendix includes the following sections:

- Regulatory Standards Compliance
- Canadian Radio Frequency Emissions Statement
- FCC Class A
- CISPR 22 (EN 55022) Class A
- VCCI

# Regulatory Standards Compliance

The following regulatory agencies have approved the Secure Content Accelerator and have found it to be fully compliant with their environmental, safety, and emissions standards.

*Table F-1 Regulatory Standards Compliance*

Regulatory Standards Compliance	Regulatory Agency
Safety	<ul style="list-style-type: none"> <li>• UL 1950 3rd, CSA NRTL</li> <li>• CAN/CSA- C22.2 No 950-M95, CSA</li> <li>• EN60950</li> <li>• TUV GS Mark</li> </ul>
EMC	<ul style="list-style-type: none"> <li>• FCC Part 15</li> <li>• EN55022</li> <li>• EN55024</li> <li>• VCCI</li> </ul>
Factory Approvals	<ul style="list-style-type: none"> <li>• UL</li> <li>• TUV</li> </ul>

## Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.



# FCC Class A

**Note**

---

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

---

To maintain compliance with the limits of a Class A digital device, Cisco requires that you use quality interface cables when connecting to this device. During testing for certification Category 5 cables were used.

**Caution**

---

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

---

The user may find the following booklet prepared by the Federal Communications Commission helpful: The Interference Handbook. This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

For more information regarding the above statement, please contact Cisco Systems, Inc.; 170 West Tasman Drive; San Jose, CA 95134-1706 USA; telephone (408) 536-4000.

# CISPR 22 (EN 55022) Class A



Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## VCCI

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。



---

## B

**Backend Server** Secure server responsible for offloading SSL processing for the client. A backend server listens for clear text from the client, encrypts the data, and connects via SSL to the server.

---

## C

**Certificate** Digital information that proves the identify of the server; similar to a digital ID card. Certificates are issued by Certificate Authorities.

**Cipher** An encryption algorithm.

---

## F

**Flash memory** Memory area in which device configuration may be saved; configuration information not stored in the flash memory is lost during a power cycle or when the device is rebooted or reloaded.

---

**K**

- Key** A cipher used to encrypt and decrypt information. Two types of keys are used: public and private. Public keys are shared; private keys are not. Public and private keys work together: information encrypted by the public key can be decrypted only by the private key.
- Key Strength** The length of a key, expressed in bits, e.g., 56 or 128. The greater the number of bits, the stronger the key.

---

**L**

- Load Balancing** Distributing network traffic evenly over two or more servers to provide better response times and reduce server overload.
- Logical Secure Server** The SSL configuration consisting of an IP address for the hardware web server providing content, an SSL TCP service port specification, a clear text port specification, a key association specifying the key and certificate to use when processing transactions, and a security policy specifying the cryptographic scheme(s) to use.

---

**R**

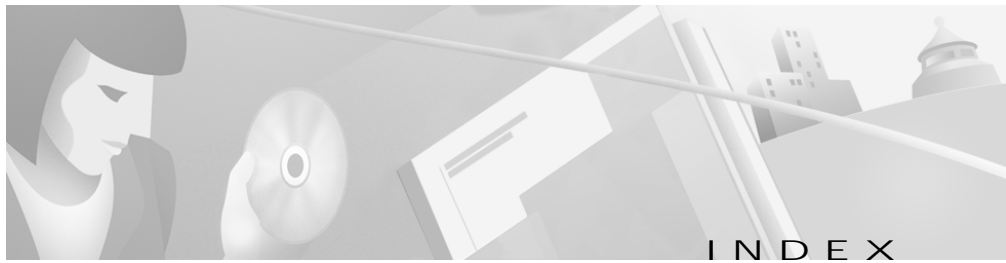
- Remote Port** The user-specified non-secure TCP port used by the Cisco Secure Content Accelerator to send decrypted data to and receive data to be encrypted from the logical secure server.
- Reverse-Proxy Server** A secure server responsible for offloading SSL processing for the client. The client browser is configured to use the IP address of the reverse-proxy server as a proxy. The reverse-proxy server is set to listen for clear text on the specified port (usually 81 or 8080). DNS information must be configured on the reverse-proxy server.

---

## S

<b>Secure Sockets Layer (SSL)</b>	An application-level protocol enabling secure transactions of data through privacy, authentication, and data integrity.
<b>Simple Network Management Protocol (SNMP)</b>	An application-level protocol used to monitor and perform basic configuration of network devices.
<b>Server Port</b>	The user-specified secure TCP port monitored by the Cisco Secure Content Accelerator for secure transaction requests.





---

## A

- access list **4-4, C-7, C-88, E-8**
  - configuration manager example **4-22**
  - GUI example **5-13**
- ambient temperature **2-4**
- Apache mod\_SSL **E-5**
- ApacheSSL **E-5**
- ARP **C-23**

---

## B

- backend server
  - backend server configuration command set **C-130**
  - configuration manager example **4-15, 4-16**
  - configuring with GUI **5-32**
- browser support **5-2**

---

## C

- cables
  - cable type **2-9**
  - Category 5 **2-9**

## caution

- ACL and static route configuration **B-24**
- connecting Network and Server ports **2-9**
- factory default reset **4-4, C-7, E-8**
- FailSafe password **6-5**
- reloading the device **3-16, 5-16**
- unauthorized modifications **17**
- unsecured transmissions **C-134, C-177**
- use of keys and certificates **6-2**

## certificate groups

- importing **4-26**

## certificate

- certificate configuration command set **C-141**
- configuration manager example **4-13**
- default **3-10**
- exporting **E-4**
- file formats **E-9**
- generating a certificate with the CLI **4-30**
- generating with GUI **5-40**
- GUI example **5-23**
- loading **3-9**
- naming conventions **3-10, 4-13, E-4**
- QuickStart wizard **3-9**
- step-up **4-23**
- step-up and server-gated cryptography **E-10**

- using existing E-4
- See also* certificate chain
- certificate chain
  - configuration manager example 4-24
  - description 4-24, E-10
  - GUI example 5-32
  - See also* certificate
- certificate group
  - certificate group configuration command set C-145
  - importing with GUI 5-44, 5-45
- Cisco Secure Content Accelerator
  - configuration commands C-1
  - configuration manager 4-1
  - description 1-2
  - free-standing installation 2-4
  - front panel 2-5
  - grounding 2-4
  - installation 2-3
  - LED descriptions 2-6
  - mounting brackets 2-5
  - QuickStart wizard configuration 3-1
  - rack-mounted installation 2-5
  - rear panel 2-6
  - unpacking 2-3
  - website configuration B-31
- client authentication
  - certgroup clientauth** command in server configuration command set C-168
  - clientauth enable** command in server configuration command set C-169
  - clientauth error** command in server configuration command set C-170
  - clientauth verifydepth** command in server configuration command set C-171
  - configuring with CLI 4-29
  - GUI example 5-31
- client IP accounting B-16
- completion features C-3
- configuration
  - QuickStart wizard 3-1
- configuration manager
  - backend server configuration command set C-130
  - certificate configuration command set C-141
  - certificate group configuration command set C-145
  - completion fixture C-3
  - configuration command set C-87
  - input data format C-2
  - interface configuration command set C-118
  - key association configuration command set C-148
  - reverse-proxy server configuration command set C-153
  - security policy configuration command set C-161
  - server configuration command set C-167
  - SNMP commands C-102
  - SSL configuration command set C-120
  - using 4-1



- configuring
  - access list 4-22
  - access lists with GUI 5-13
  - adding a route with GUI 5-10
  - backend server 4-15, 4-16
  - backend server with GUI 5-32
  - certificate 3-9, 4-13
  - certificate chain 4-24
  - certificate chain with GUI 5-32
  - certificate with GUI 5-23
  - clear text and SSL ports E-2
  - client authentication with GUI 5-31
  - client-side Web access 5-4
  - device name with GUI 5-6
  - enabling RIP with GUI 5-9
  - encrypted management sessions 4-20
  - Ethernet interface 4-23
  - Ethernet interface with GUI 5-8
  - generating a certificate 4-30
  - generating a key with CLI 4-30
  - group configuration command set C-85
  - GUI 5-1, 6-1, C-8, E-12
  - importing a certificate group with GUI 5-44, 5-45
  - key 3-8, 4-13
  - key with GUI 5-21
  - management method comparison C-8, E-12
  - non-privileged command set C-15
  - other secure protocols 4-32, 5-35
  - password 3-12
  - privileged command set C-63
  - QuickStart wizard 3-1
  - reloading with GUI 5-16
  - remote configuration manager C-8, E-12
  - reverse-proxy server with GUI 5-32
  - RIP 4-32
  - secure server 4-12
  - secure server with GUI 5-21, 5-29
  - Secure Server wizard in GUI 5-46
  - security policy 3-11, 4-14, 4-15, 4-16
  - security policy with GUI 5-26
  - serial connection C-8, E-12
  - setting an enable password with GUI 5-16
  - setting device IP address with GUI 5-7
  - setting syslog hosts with GUI 5-12
  - SNMP 4-31
  - SNMP with GUI 5-18
  - SNTP servers 4-19
  - telnet connection C-8, E-12
  - top level command set C-15
  - URL rewrite 4-17
  - See also* example
- configuring with CLI
  - client authentication 4-29
  - server authentication 4-27
- cryptographic algorithm
  - table of E-10
- CSS, use with
  - examples B-3

- in-line B-4
- one-armed proxy B-16
- one-armed transparent B-22
- transparent sandwich B-8

---

## D

### deployment examples

- in-line B-4
- load balancing B-2
- one-armed proxy B-16
- one-armed transparent B-22
- single device B-2
- transparent sandwich B-8
- use with the CSS B-3

---

## E

### encrypted management

- configuration manager example 4-20
- description 4-4, C-7, E-8

### Ethernet

- configuration manager example 4-23
- connecting 2-9

### example (CLI)

- configuring client authentication 4-29
- configuring server authentication 4-27

### example, configuration manager

- access list 4-22

- configuring an Ethernet interface 4-23
- configuring a secure mail server 4-33
- configuring encrypted management sessions 4-20

- configuring RIP 4-32

- configuring SNMP 4-31

- configuring Sntp servers 4-19

- configuring URL rewrite 4-17

- enabling chained certificates 4-24

- generating a certificate 4-30

- generating a key 4-30

- setting up a backend server 4-15, 4-16

- setting up a secure server 4-12

- setting up basic device parameters

### example, GUI

- adding a route 5-10

- client authentication 5-31

- configuring access lists 5-13

- configuring a certificate 5-23

- configuring a certificate chain 5-32

- configuring a key 5-21

- configuring an Ethernet interface 5-8

- configuring a reverse-proxy server 5-32

- configuring a secure server 5-29

- configuring a security policy 5-26

- configuring backend server 5-32

- configuring other secure protocols 5-35

- configuring secure server 5-21

- configuring SNMP 5-18

- enabling RIP 5-9

- generating an RSA key 5-36
- generating a certificate 5-40
- importing a certificate group 5-44, 5-45
- reloading the device 5-16
- resetting the IP address 5-7
- setting an enable password 5-16
- setting syslog hosts 5-12
- setting the device name 5-6

---

## F

### FIPS Mode

- configuring and using 6-1
- fips enable** command C-74
- product overview 1-2
- free-standing installation 2-4
- front panel 2-5

---

## G

- gateway 3-12
- graphical user interface (GUI)
  - description C-8, E-12
- group configuration command set C-85
- GUI
  - adding a route 5-10
  - browser support 5-2
  - configuring a certificate 5-23
  - configuring a certificate chain 5-32

- configuring a key 5-21
- configuring an Ethernet interface 5-8
- configuring a reverse-proxy server 5-32
- configuring a secure server 5-21, 5-29
- configuring a security policy 5-26
- configuring backend server 5-32
- configuring client authentication 5-31
- configuring client-side access 5-4
- configuring device name 5-6
- configuring other secure protocols 5-35
- configuring SNMP 5-18
- enabling RIP 5-9
- enabling Web management 5-2
- generating a certificate 5-40
- generating an RSA key 5-36
- importing a certificate group 5-44, 5-45
- interface 5-5
- reloading the device 5-16
- resetting the IP address 5-7
- restricting Web management 5-3
- Secure Server wizard 5-46
- setting an enable password 5-16
- setting syslog hosts 5-12
- starting 5-3
- GUI (graphical user interface)
  - configuration with 5-1

## I

IIS 4 on Windows NT E-5  
 IIS 5 E-6  
 importing certificate groups 4-26  
 input data format C-2

## K

## key

configuration manager example 4-13  
 default 3-9  
 exporting E-4  
 file formats E-9  
 generating a key with the CLI 4-30  
 generating with **genrsa** command C-149  
 generating with GUI 5-36  
 GUI example 5-21  
 key association configuraiton command set C-148  
 loading 3-8  
 naming conventions 3-9, 4-13, E-4  
 QuickStart wizard 3-8  
 using existing E-4

## L

LED descriptions 2-6  
 Linux  
 remote configuration manager 3-4, 4-7, C-11

software 2-10  
 softwre 1-4

## M

management session  
 initiating 3-2, 4-5, C-10  
 mounting brackets 2-5

## N

network deployment  
 in-line B-4  
 load balancing B-2  
 one-armed transparent B-22  
 single device B-2  
 transparent sandwich B-8  
 use with the CSS B-3  
 non-privileged command set C-15

## O

**on** prefix 4-9, C-13  
 operating systems 1-4

## P

password  
 access 4-3, C-6, E-7

- description 4-3, C-6, E-7
  - enable 4-3, 5-16, C-6, E-7
  - FailSafe 4-4, C-7, E-8
  - setting with QuickStart wizard 3-12
- PCKS7 file importing 4-26
- platforms 1-4
- port blocking E-2
- power cords
- connecting 2-7
- power supply
- ensuring availability 2-8
  - LEDs 2-7
- privileged command set C-63
- 
- Q**
- QuickStart wizard
- description C-9, E-13
  - starting 3-5
  - using 3-1
  - using with configured appliance 3-16
- 
- R**
- rack-mounted installation 2-5
- rear panel 2-6
- remote configuration manager
- caching 4-10, C-14
  - description C-8, E-12
  - device groups 4-9, C-13
  - initiating a management session 3-4, 4-7, C-11
  - Linux 3-4, 4-7, C-11
  - on** prefix 4-9, C-13
  - Solaris 3-4, 4-7, C-11
  - specifying devices 4-8, C-12
  - using 4-8, C-12
  - using the QuickStart wizard 3-6
  - Windows 2000 3-4, 4-7, C-12
  - Windows NT 3-4, 4-7, C-12
- requirements
- installation tools and equipment 2-2
  - site planning 2-2
- resetting to factory defaults 4-4, C-7, E-8
- reverse-proxy server
- configuring with GUI 5-32
  - reverse-proxy server configuration command set C-153
- RIP 4-32, C-38, C-101
- 
- S**
- secure management
- See also* encrypted management
- secure server
- configuration manager example 4-12
  - description E-9
  - GUI example 5-21, 5-29
  - naming conventions 3-7
  - server configuration command set C-167

- Secure Server wizard 5-46
- secure URL rewrite
  - product overview 1-2
- security policy
  - configuration manager example 4-14, 4-15, 4-16
  - cryptographic algorithms (table) E-10
  - default 3-11
  - description E-10
  - GUI example 5-26
  - naming conventions 4-14
  - QuickStart wizard 3-11
  - security policy configuration command set C-161
- serial connection
  - description C-8, E-12
  - initiating a management session 3-2, 4-5, C-10
  - symbolic hostnames C-9, E-12
  - terminal settings 3-3, 4-6, C-10
  - using the QuickStart wizard 3-5
- server authentication
  - certgroup serverauth** command in backend server configuration command set C-130
  - certgroup serverauth** command in reverse-proxy server configuration command set C-153
  - configuring with CLI 4-27
  - serverauth enable** command in backend server configuration command set C-135
  - serverauth enable** command in reverse-proxy configuration command set C-157
  - serverauth ignore** command in backend server configuration command set C-136
  - serverauth ignore** command in reverse-proxy server configuration command set C-158
- shipment contents 2-2
- site requirements 2-2
- SNMP
  - commands C-79
  - configuration commands C-102
  - configuration manager example 4-31
  - GUI example 5-18
  - MIB-II support 1-2
- SNTP
  - product overview 1-2
- SNTP servers
  - configuration manager example 4-19
- software
  - Linux 1-4, 2-10
  - Solaris 2-10
  - Windows 2000 1-4, 2-11
  - Windows NT 1-4, 2-11
- Solaris
  - remote configuration manager 3-4, 4-7, C-11
  - software 2-10
- specifications
  - electrical A-2

environmental **A-2**  
 physical **A-3**

SSL

- Cisco configuration components **E-9**
- GUI examples **5-21**
- introduction **E-2**
- versions supported **1-3**

SSL commands **C-120**

- backend server configuraiton command set **C-130**
- certificate configuration command set **C-141**
- certificate group configuration command set **C-145**
- key association configuration command set **C-148**
- reverse-proxy server configuraiton command set **C-153**
- security policy configuration command set **C-161**
- server configuration command set **C-167**

SSL configuration command set **C-120**

Stronghold **E-5**

---

## T

telnet connection

- description **C-8, E-12**
- initiating a managment session **3-3, 4-7, C-11**
- symbolic hostnames **C-9, E-12**
- using the QuickStart wizard **3-5**

terminal settings **3-3, 4-6, C-10**

text conventions **xxxiii, C-2**

tools for installation **2-2**

top level command set **C-15**

troubleshooting **D-2**

---

## U

URL rewrite

- configuration manager example **4-17**

---

## W

warning

- CISPR 22 (EN 55022) Class A **18**
- equipment rack stability **2-5**
- grounding **2-4**
- power systems **A-2**
- shock hazard **2-3, 2-4**
- site requirement **2-2**

Web management

- configuring client-side access **5-4**
- enabling **5-2**
- restricting access **5-3**
- See also* GUI

website configuration **B-31**

Windows 2000

- IIS 5 **E-6**
- remote configuration manager **3-4, 4-7, C-12**
- software **1-4, 2-11**

Windows NT

IIS 4 E-5

remote configuration manager 3-4, 4-7, C-12

software 1-4, 2-11