



About This Guide

This preface describes who should read the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*, how it is organized, and its document conventions. This preface includes the following sections:

- [Document Objectives, page xxxiii](#)
- [Audience, page xxxiii](#)
- [Document Organization, page xxxiv](#)
- [Document Conventions, page xxxv](#)
- [Related Documentation, page xxxvi](#)
- [Obtaining Documentation, page xxxvi](#)
- [Documentation Feedback, page xxxvii](#)
- [Cisco Product Security Overview, page xxxvii](#)
- [Obtaining Technical Assistance, page xxxviii](#)
- [Obtaining Additional Publications and Information, page xl](#)

Document Objectives

This guide contains the commands available for use with the FWSM to protect your network from unauthorized use.

You can also configure and monitor the FWSM by using ASDM, a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online Help for less common scenarios. For more information, see:

<http://www.cisco.com/univercd/cc/td/doc/product/netsec/secgmt/asdm/index.htm>.

Audience

This publication is for experienced network administrators who are responsible for managing network security, configuring firewalls, managing default and static routes, and managing TCP and UDP services. Use this guide with the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

Document Organization

This guide includes the following chapters:

- Chapter 1, “Using the Command-Line Interface,” introduces you to the FWSM commands and access modes.
- Chapter 2, “aaa accounting through accounting-server-group Commands,” provides detailed descriptions of the **aaa accounting** through **accounting-server-group** commands.
- Chapter 3, “activation-key through auto-update timeout Commands,” provides detailed descriptions of the **activation-key** through **auto-update timeout** commands.
- Chapter 4, “backup-servers through bridge-group Commands,” provides detailed descriptions of the **backup-servers** through **bridge-group** commands.
- Chapter 5, “cache-time through clear capture Commands,” provides detailed descriptions of the **cache-time** through **clear capture** commands.
- Chapter 6, “clear configure through clear configure virtual Commands,” provides detailed descriptions of the **clear configure** through **clear configure virtual** commands.
- Chapter 7, “clear console-output through clear xlate Commands,” provides detailed descriptions of the **clear console-output** through **clear xlate** commands.
- Chapter 8, “client-access-rule through cri-configure Commands,” provides detailed descriptions of the **client-access-rule** through **cri-configure** commands.
- Chapter 9, “crypto ca authenticate through crypto map set trustpoint Commands,” provides detailed descriptions of the **crypto ca authenticate** through **crypto map set trustpoint** commands.
- Chapter 10, “debug aaa through debug sip Commands,” provides detailed descriptions of the **debug aaa** through **debug sip** commands.
- Chapter 11, “default through drop Commands,” provides detailed descriptions of the **default** through **drop** commands.
- Chapter 12, “email through ftp-map Commands,” provides detailed descriptions of the **email** through **ftp-map** commands.
- Chapter 13, “gateway through http-map Commands,” provides detailed descriptions of the **gateway** through **http-map** commands.
- Chapter 14, “icmp through ignore lsamospf Commands,” provides detailed descriptions of the **icmp** through **ignore lsamospf** commands.
- Chapter 15, “inspect ctiqbe through inspect xdmcp Commands,” provides detailed descriptions of the **inspect ctiqbe** through **inspect xdmcp** commands.
- Chapter 16, “interface through issuer-name Commands,” provides detailed descriptions of the **interface** through **issuer-name** commands.
- Chapter 17, “join-failover-group through kill Commands,” provides detailed descriptions of the **join-failover-group** through **kill** commands.
- Chapter 18, “ldap-base-dn through log-adj-changes Commands,” provides detailed descriptions of the **ldap-base-dn** through **log-adj-changes** commands.
- Chapter 19, “logging asdm through logout Commands,” provides detailed descriptions of the **inspect ctiqbe** through **inspect xdmcp** commands.
- Chapter 20, “mac-address-table aging-time through multicast-routing Commands,” provides detailed descriptions of the **mac-address-table** through **multicast-routing** commands.

- Chapter 21, “name through ospf transmit-delay Commands,” provides detailed descriptions of the **name** through **ospf transmit-delay** commands.
- Chapter 22, “pager through pwd Commands,” provides detailed descriptions of the **passwd** through **pwd** commands.
- Chapter 23, “queue-limit through router-id Commands,” provides detailed descriptions of the **queue-limit** through **router-id** commands.
- Chapter 24, “same-security-traffic through show asdm sessions Commands,” provides detailed descriptions of the **same-security-traffic** through **show asdm sessions** commands.
- Chapter 25, “show asp drop through show curpriv Commands,” provides detailed descriptions of the **show asp drop** through **show curpriv** commands.
- Chapter 26, “show debug through show ipv6 traffic Commands,” provides detailed descriptions of the **show debug** through **show ipv6 traffic** commands.
- Chapter 27, “show isakmp sa through show route Commands,” provides detailed descriptions of the **show isakmp sa** through **show route** commands.
- Chapter 28, “show running-config through show running-config isakmp Commands,” provides detailed descriptions of the **show running-config** through **show running-config isakmp** commands.
- Chapter 29, “show running-config logging through show running-config vpn-sessiondb Commands,” provides detailed descriptions of the **show running-config logging** through **show running-config vpn-sessiondb** commands.
- Chapter 30, “show service-policy through show xlate Commands,” provides detailed descriptions of the **show service-policy** through **show xlate** commands.
- Chapter 31, “shun through sysopt uauth allow-http-cache Commands,” provides detailed descriptions of the **shun** through **sysopt uauth allow-http-cache** commands.
- Chapter 32, “tcp-map through tunnel-limit Commands,” provides detailed descriptions of the **tcp-map** through **tunnel-limit** commands.
- Chapter 33, “upgrade-mp through write terminal Commands,” provides detailed descriptions of the **upgrade-mp** through **write terminal** commands.

Document Conventions

The FWSM command syntax descriptions use the following conventions:

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in *screen* font.
- Information you need to enter in examples is shown in **boldface screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

- Examples might include output from different platforms; for example, you might not recognize an interface type in an example because it is not available on your platform. Differences should be minor.

**Note**

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

For information on modes, prompts, and syntax, see [Chapter 1, “Using the Command-Line Interface.”](#)

Related Documentation

For more information, refer to the following documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*
- *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Release Notes*
- *Cisco ASDM Release Notes*

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

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

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



Tip

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

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

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

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

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

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

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

