



Selective Enabling of Applications Using an HTTP or HTTPS Server

The Selective Enabling of Applications Using an HTTP or HTTPS Server feature eliminates a potential security vulnerability by providing a facility to enable selected HTTP and HTTP over Secure Socket Layer (HTTPS) services on both the Cisco IOS HTTP and HTTPS server infrastructure. This feature also provides the capability to view the current state of the HTTP and HTTPS services, including which services are enabled or disabled.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Selective Enabling of Applications Using an HTTP or HTTPS Server” section on page 7](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About Selective Enabling of Applications Using an HTTP or HTTPS Server, page 2](#)
- [How to Enable Selected Applications Using an HTTP or HTTPS Server, page 2](#)
- [Configuration Examples for Selective Enabling of Applications Using an HTTP or HTTPS Server, page 5](#)
- [Additional References, page 5](#)



Information About Selective Enabling of Applications Using an HTTP or HTTPS Server

To use the Selective Enabling of Applications Using an HTTP or HTTPS Server feature, you should understand the following concept:

- [Selective Enabling of Applications Within the HTTP and HTTPS Infrastructure, page 2](#)

Selective Enabling of Applications Within the HTTP and HTTPS Infrastructure

The Selective Enabling of Applications Using an HTTP or HTTPS Server feature eliminates a potential security vulnerability by providing a facility to enable selected HTTP and HTTPS services on both the Cisco IOS HTTP and HTTPS server infrastructure. This feature also provides the capability to view the current state of the HTTP and HTTPS services, including which services are enabled or disabled.

Prior to this feature, HTTP or HTTPS applications running on a router or a switch, were either all enabled or all disabled when the HTTP server or HTTPS server was enabled or disabled, respectively (using the **ip http server** and **ip http secure-server** commands). In the situation where all HTTP or HTTPS applications were enabled, remote end-users were given potential access to services that could allow them to pose a potential security threat to service providers.

With this new feature, the Cisco IOS HTTP and HTTPS infrastructure provides a way to enable only selected HTTP and HTTPS applications to run on a router or a switch, thereby bypassing a potential security vulnerability. Selected HTTP and HTTPS applications can be enabled using the new **ip http active-session-modules** and **ip http secure-active-session-modules** configuration commands, respectively.

**Note**

The maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

How to Enable Selected Applications Using an HTTP or HTTPS Server

This section contains the following procedures:

- [Enabling Selected HTTP Applications, page 2](#)
- [Enabling Selected HTTPS Applications, page 3](#)

Enabling Selected HTTP Applications

Perform this task to selectively enable the HTTP applications that will service incoming HTTP requests from remote clients.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. `ip http session-module-list listname prefix1 [prefix2,..., prefixn]`
4. `ip http active-session-modules {listname | none | all}`
5. `end`
6. `show ip http server session-module`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>ip http session-module-list listname prefix1 [prefix2,...,prefixn]</code></p> <p>Example: Router(config)# ip http session-module-list list1 SCEP,HOME_PAGE</p>	<p>Defines a list of HTTP or HTTPS application names.</p>
Step 4	<p><code>ip http active-session-modules {listname none all}</code></p> <p>Example: Router(config)# ip http active-session-modules list1</p>	<p>Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.</p> <ul style="list-style-type: none"> • The <i>listname</i> argument enables only those HTTP services configured in the list identified by the <code>ip http session-module-list</code> command to serve HTTP requests. • The keyword none disables all HTTP services from serving HTTP requests. • The keyword all enables all HTTP services to serve HTTP requests.
Step 5	<p><code>end</code></p> <p>Example: Router(config)# end</p>	<p>Ends your configuration session and returns the CLI to Privileged Exec mode.</p>
Step 6	<p><code>show ip http server session-module</code></p> <p>Example: Router# show ip http server session-module</p>	<p>(Optional) Displays information about all HTTP and HTTPS services available on the router or switch, including their current state of service, such as whether they are enabled or disabled.</p>

Enabling Selected HTTPS Applications

Perform this task to selectively enable the HTTPS applications that will service incoming HTTPS requests from remote clients.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http session-module-list** *listname prefix1* [*prefix2*,..., *prefixn*]
4. **ip http secure-active-session-modules** {*listname* | **none** | **all**}
5. **end**
6. **show ip http server session-module**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http session-module-list <i>listname prefix1</i> [<i>prefix2</i> ,..., <i>prefixn</i>] Example: Router(config)# ip http session-module-list list1 SCEP,HOME_PAGE	Defines a list of HTTP or HTTPS application names.
Step 4	ip http secure-active-session-modules { <i>listname</i> none all }	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients. <ul style="list-style-type: none"> • The <i>listname</i> argument enables only those HTTPS services configured in the list identified by the ip http session-module-list command to serve HTTPS requests. • The keyword none disables all HTTPS services from serving HTTPS requests. • The keyword all enables all HTTPS services to serve HTTPS requests.
Step 5	end Example: Router(config)# end	Ends your configuration session and returns the CLI to Privileged Exec mode.
Step 6	show ip http server session-module Example: Router# show ip http server session-module	(Optional) Displays information about all HTTP and HTTPS services available on the router or switch, including their current state of service, such as whether they are enabled or disabled.

Configuration Examples for Selective Enabling of Applications Using an HTTP or HTTPS Server

This section provides the following configuration example:

- [Enabling Selected HTTP and HTTPS Applications: Example, page 5](#)

Enabling Selected HTTP and HTTPS Applications: Example

The following configuration sample shows a configuration with different set of services available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Additional References

The following sections provide references related to the Selective Enabling of Applications Using an HTTP or HTTPS Server feature.

Related Documents

Related Topic	Document Title
Additional HTTP configuration information	Using the Cisco Web Browser User Interface feature module
Additional HTTPS configuration information	HTTPS - HTTP Server and Client with SSL 3.0 feature module
Additional HTTP and HTTPS commands	Cisco IOS Network Management Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for Selective Enabling of Applications Using an HTTP or HTTPS Server

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Selective Enabling of Applications Using an HTTP or HTTPS Server

Feature Name	Releases	Feature Information
Selective Enabling of Applications Using an HTTP or HTTPS Server	12.3(14)T	The Selective Enabling of Applications Using an HTTP or HTTPS Server feature eliminates a potential security vulnerability by providing a facility to enable selected HTTP and HTTP over Secure Socket Layer (HTTPS) services on both the Cisco IOS HTTP and HTTPS server infrastructure. This feature also provides the capability to view the current state of the HTTP and HTTPS services, including which services are enabled or disabled.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynx, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

