



Selective Enabling of Applications Using an HTTP or HTTPS Server

HTTP Server - Enabling of Applications

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.

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

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

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](#)
- [Command Reference, page 6](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

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	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 [prefix2,...,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 active-session-modules { <i>listname</i> none all } Example: Router(config)# ip http active-session-modules list1	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients. <ul style="list-style-type: none"> • The <i>listname</i> argument enables only those HTTP services configured in the list identified by the ip http session-module-list 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	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.

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,...,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” chapter in the section “Cisco IOS User Interfaces” in the <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> , Release 12.3T
Additional HTTPS configuration information	HTTPS - HTTP Server and Client with SSL 3.0 , Cisco IOS Release 12.2(15)T feature module.
Additional HTTP and HTTPS commands	Cisco IOS Configuration Fundamentals and Network Management Command Reference , Release 12.3T

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
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands only.

- [ip http active-session-modules](#)
- [ip http secure-active-session-modules](#)
- [ip http session-module-list](#)
- [show ip http server](#)

ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command in global configuration mode. Use the **no** form of this command to return to the default, which is that all HTTP services will be enabled.

```
ip http active-session-modules {listname | none | all}
```

```
no ip http active-session-modules {listname}
```

Syntax Description

<i>listname</i>	Enables only those HTTP services configured in the list identified by the ip http session-module-list command to serve HTTP requests. All other HTTP or HTTPS applications on the router or switch will be disabled.
none	Disables all HTTP services.
all	Enables all HTTP applications to service incoming HTTP requests from remote clients.

Defaults

If no arguments or keywords are specified, all HTTP services will be enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or HTTPS application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

Examples

The following example shows how to configure a different set of services to be 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
```

Related Commands	Command	Description
	ip http secure-active-session- modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
	ip http session-module-list	Defines a list of HTTP or HTTPS application names.
	show ip http server	Displays details about the current configuration of the HTTP server.

ip http secure-active-session-modules

To selectively enable HTTPS applications for servicing incoming HTTPS requests from remote clients, use the **ip http secure-active-session-modules** command in global configuration mode. Use the **no** form of this command to return to the default, which is that all HTTPS services will be enabled.

ip http secure-active-session-modules {*listname* | **none** | **all**}

no ip http secure-active-session-modules

Syntax Description

<i>listname</i>	Enables only those HTTPS services configured in the list identified by the ip http session-module-list command to serve HTTPS requests. All other HTTP or HTTPS applications on the router or switch will be disabled.
none	Disables all HTTPS services.
all	Enables all HTTPS applications to service incoming HTTPS requests from remote clients.

Defaults

If no arguments or keywords are specified, all HTTPS services will be enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ip http secure-active-session-modules** command to selectively enable HTTPS applications, for servicing incoming HTTPS requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or HTTPS application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

Examples

The following example shows how to configure a different set of services to be 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
```

Related Commands	Command	Description
	ip http active-session-modules	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.
	ip http session-module-list	Defines a list of HTTP or HTTPS application names.
	show ip http server	Displays details about the current configuration of the HTTP server.

ip http session-module-list

To define a list of HTTP or HTTPS application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

```
ip http session-module-list listname prefix1 [prefix2,...,prefixn]
```

```
no ip http session-module-list listname prefix1 [prefix2,...,prefixn]
```

Syntax Description		
<i>listname</i>	Name of the list.	
<i>prefix1</i>	Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE.	
<i>prefix2,...,prefixn</i>	(Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma.	

Defaults No list of HTTP or HTTPS application names is defined.

Command Modes Global configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a router or switch. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

Examples The following example shows how to configure a different set of services to be 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 session-module-list

```
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http active-session-modules	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
show ip http server	Displays details about the current configuration of the HTTP server.

show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in user EXEC or privileged EXEC mode.

show ip http server {all | status | session-module | connection | statistics | history}

Syntax Description

all	Displays all HTTP server information.
status	Displays only HTTP server status configuration.
session-module	Displays only supported HTTP services (Cisco IOS modules).
connection	Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.
statistics	Displays only HTTP server connection statistics.
history	Displays only the previous 20 connections to the HTTP server, including the IP address accessed, and the time when the connection was closed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(14)T	The display for the session-module keyword was updated with the Status and Secure-Status fields.

Usage Guidelines

Use this command to show detailed status information about the HTTP server.

If the HTTP secure server capability is present, the output of the **show ip http server all** command will also include the information found in the output of the **show ip http server secure status** command.

Examples

The following is sample output from the **show ip http server all** command:

```
Router# show ip http server all

HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 30 seconds
Server life time-out: 120 seconds
Maximum number of requests allowed on a connection: 2
HTTP secure server capability: Not Present
HTTP server application session modules:
  Session module Name  Handle  Description
Homepage_Server      5       IOS Homepage Server
```

show ip http server

```

QDM                2          QOS Device Manager Server
HTTP IFS Server    1          HTTP based IOS File Server
QDM SA             3          QOS Device Manager Signed Applet Server
WEB_EXEC           4          HTTP based IOS EXEC Server
XSM                6          XML Session Manager
VDM                7          VPN Device Manager Server
ITS                8          IOS Telephony Service
ITS_LOCDIR         9          ITS Local Directory Search

HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
  172.19.254.37:80    128.190.254.45:33737  70        2294

HTTP server statistics:
Accepted connections total: 1360

HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
  172.91.254.37:80    128.190.254.45:63530  60        1596      10:50:00 12/19

```

Table 1 describes the significant fields shown in the display.

Table 1 show ip http server all Field Descriptions

Field	Description
HTTP server status:	Enabled or disabled. Corresponds to the [no] ip http server command.
HTTP server port:	Port used by the HTTP server. Corresponds to the ip http port command.
HTTP server authentication method:	Authentication method used for HTTP server logins. Corresponds to the ip http authentication command.
HTTP server access class:	Access list number assigned to the HTTP server. A value of zero (0) indicates no access list is assigned. Corresponds to the ip http access-class command.
HTTP server base path:	Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the ip http path command.
Maximum number of concurrent server connections allowed:	Corresponds to the ip http max-connections command.
Server idle time-out:	The maximum number of seconds the connection will be kept open if no data is received or if response data cannot be sent out. Corresponds to the ip http timeout-policy command.
Server life time-out:	The maximum number of seconds the connection will be kept open. Corresponds to the ip http timeout-policy command.
Maximum number of requests allowed on a connection:	The maximum number of requests that will be processed on a connection before the connection is closed. Corresponds to the ip http timeout-policy command.
HTTP secure server capability:	Indicates if the running software image supports the HTTPS server ("Present" or "Not Present"). If the capability is present, the output from the show ip http server secure status command will appear after this line.

Table 1 *show ip http server all Field Descriptions (continued)*

Field	Description
HTTP server application session modules:	<p>Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including:</p> <ul style="list-style-type: none"> the Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server the VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM) the QoS Device Manager (QDM) application, which uses the QDM Server the IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS)
HTTP server current connections:	Currently active HTTP connections.
HTTP server statistics:	How many connections have been accepted.
HTTP server history:	<p>Details about the last 20 connections, including the time the connection was closed (end-time). End-time is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format:</p> <p><i>hh:mm:ss month/day</i></p>

The following is sample output from the **show ip http server status** command:

```
Router# show ip http server status
```

```
HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 600 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

The lines indicating the status of the HTTP secure (HTTPS) server will only be visible if your software image supports the HTTPS server. If your software image does not support SSL, only the following line will be visible:

```
HTTP secure server capability: Not present
```

The following is sample output from the **show ip http server session-module** command:

```
Router(config)# show ip http server session-module

HTTP server application session modules:
Session module Name Handle Status Secure-status Description
HOME_PAGE           4 Active Active IOS Homepage Server
HTTP_IFS            1 Active
Active HTTP based IOS File Server
IXI                  2 Active Active IOS XML Infra Application Server
WEB_EXEC            3 Active
Active HTTP based IOS EXEC Server
QDM                  5 Active Active QOS Device Manager Server
QDM_SA              6 Active
Active QOS Device Manager Signed Applet Server
XSM                  7 Active Active XML Session Manager
VDM                  8 Active
Active VPN Device Manager Server
XML_Api             9 Active Active XML Api
ITS                  10
Active Active IOS Telephony Service
ITS_LOCDIR          11 Active Active ITS Local Directory Search
tti-petitioner      12 Active
Active TTI Petitioner
Router(config)#
```

Related Commands

Command	Description
debug ip http server all	Enables debugging output for all HTTP processes on the system.
ip http secure-server	Enables the secure HTTP (HTTPS) server.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.
show ip http server secure status	Displays the status of the secure HTTP (HTTPS) server.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.
This document first published March 28, 2005. Last updated: March 28, 2005.