



# 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, page 1](#)
- [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 for Selective Enabling of Applications Using an HTTP or HTTPS Server, page 6](#)
- [Feature Information for Selective Enabling of Applications Using an HTTP or HTTPS Server, page 7](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

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

## 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

### 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** *list-name prefix-1 [prefix-2,...,prefix-n]*
4. **ip http active-session-modules** {*list-name* | **none** | **all**}
5. **end**
6. **show ip http server session-module**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip http session-module-list</b> <i>list-name prefix-1 [prefix-2,...,prefix-n]</i>  <b>Example:</b> Router(config)# ip http session-module-list list1 SCEP,HOME_PAGE	Defines a list of HTTP or HTTPS application names.
<b>Step 4</b>	<b>ip http active-session-modules</b> { <i>list-name</i>   <b>none</b>   <b>all</b> }  <b>Example:</b> 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"> <li>• The <i>listname</i> argument enables only those HTTP services configured in the list identified by the <b>ip http session-module-list</b> command to serve HTTP requests.</li> <li>• The keyword <b>none</b> disables all HTTP services from serving HTTP requests.</li> <li>• The keyword <b>all</b> enables all HTTP services to serve HTTP requests.</li> </ul>
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Router(config)# end	Ends your configuration session and returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ip http server session-module</b>  <b>Example:</b> 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** *list-name prefix-1 [prefix-2,...,prefix-n]*
4. **ip http secure-active-session-modules** {*list-name* | **none** | **all**}
5. **end**
6. **show ip http server session-module**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip http session-module-list</b> <i>list-name prefix-1 [prefix-2,...,prefix-n]</i>  <b>Example:</b> Router(config)# ip http session-module-list list1 SCEP,HOME_PAGE	Defines a list of HTTP or HTTPS application names.
<b>Step 4</b>	<b>ip http secure-active-session-modules</b> { <i>list-name</i>   <b>none</b>   <b>all</b> }	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.  <ul style="list-style-type: none"> <li>• The <i>listname</i> argument enables only those HTTPS services configured in the list identified by the <b>ip http session-module-list</b> command to serve HTTPS requests.</li> <li>• The keyword <b>none</b> disables all HTTPS services from serving HTTPS requests.</li> <li>• The keyword <b>all</b> enables all HTTPS services to serve HTTPS requests.</li> </ul>

	Command or Action	Purpose
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Router(config)# end	Ends your configuration session and returns the CLI to Privileged Exec mode.
<b>Step 6</b>	<b>show ip http server session-module</b>  <b>Example:</b> 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

### Example: Enabling Selected HTTP and HTTPS Applications

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
```

### Example: Verifying HTTP and HTTPS Applications

The following example shows how to list the HTTP and HTTPS applications that have been selectively enabled or disabled using the **ip http session-module-list list-name prefix-1 [prefix-2,...,prefix-n]** command:

```
Device# show ip http server session-module
```

```
HTTP server application session modules:
Session module Name  Handle Status  Secure-status  Description
HOME_PAGE            2       Active  Active        IOS Homepage Server
GSI3D3FD3DC-wsma     6       Active  Active        wsma infra
HTTP_IFS              1       Active  Active        HTTP based IOS File Server
BANNER_PAGE          3       Active  Active        HTTP Banner Page Server
WEB_EXEC              4       Active  Active        HTTP based IOS EXEC Server
IXI                   5       Active  Active        IOS XML Infra Application Server
GSI3D31BCA4-wsma     7       Active  Active        wsma infra
EXTERN                9       Active  Active        External Distributed HTTP server
dot11                 30      Active  Active        dot11
links                 31      Active  Active        links
tgconfig              32      Active  Active        tgconfig
```

system	33	Active	Active	system
javascript	34	Active	Active	javascript
css	35	Active	Active	css
images	36	Active	Active	images
wlan	37	Active	Active	wlan
wireless	38	Active	Active	wireless

**Note**

The applications that can be enabled or disabled vary based on the platform and applications that register with HTTP infra during run time. HTTP infra provides a web interface that is referred to as legacy WebUI. This WebUI provides links to the following applications:

- Diagnostic log
- HTML access to command-line interface
- Connectivity test —ping interface
- Platform utilities
- Show tech support
- Extended ping
- Any platform-specific home page
- Contact information

## Additional References for Selective Enabling of Applications Using an HTTP or HTTPS Server

### Related Documents

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

**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>	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**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.

