



HTTP 1.1 Web Server and Client

The HTTP 1.1 Web Server and Client feature provides a consistent interface for users and applications by implementing support for HTTP 1.1 in Cisco IOS software-based devices. Prior to this release, Cisco software supported an implementation of HTTP 1.0. The integrated HTTP server API supports server application interfaces. When combined with the HTTPS feature, the HTTP 1.1 Web Server and Client provides a complete, secure solution for HTTP services to and from Cisco devices.

Feature Specifications for the HTTP 1.1 Web Server and Client

Feature History

Release	Modification
11.2	The HTTP 1.0 Web Server and Cisco Web browser user interface were introduced.
12.2(15)T	The HTTP 1.1 Web Server and HTTP 1.1 Web Client were introduced.

Supported Platforms

The HTTP 1.1 Web Server and Client are supported on all Cisco IOS-based platforms. See Cisco Feature Navigator for details.

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 the HTTP 1.1 Web Server and Client, page 2](#)
- [How to Configure the HTTP 1.1 Web Server, page 3](#)
- [How to Configure the HTTP Client, page 5](#)
- [Configuration Examples for the HTTP 1.1 Web Server, page 9](#)
- [Where to Go Next, page 10](#)
- [Additional References, page 11](#)
- [Command Reference, page 12](#)

Information About the HTTP 1.1 Web Server and Client

This feature updates the Cisco implementation of the Hypertext Transfer Protocol (HTTP) from 1.0 to 1.1. The HTTP server allows features and applications, such as the Cisco Web browser user interface, to be run on your routing device.

The Cisco implementation of HTTP 1.1 is backward-compatible with previous Cisco IOS releases. If you are currently using configurations that enable the HTTP server, no configuration changes are needed, as all defaults remain the same.

The process of enabling and configuring the HTTP server also remains the same as in previous releases. Support for Server Side Includes (SSI) and HTML forms has not changed. Additional configuration options, in the form of the **ip http timeout-policy** command and the **ip http max-connections** command have been added. These options allow configurable resource limits for the HTTP server. If you do not use these optional commands, the default policies are used.

Remote applications may require that you enable the HTTP server before using them. Applications that use the HTTP server include:

- 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 uses the ITS Local Directory Search and IOS Telephony Server (ITS)

No Cisco applications make use of the HTTP Client in Cisco IOS Release 12.2(15)T.

About HTTP Server General Access Policies

The new **ip http timeout-policy** command allows you to specify general access characteristics for the server by configuring a value for idle time, connection life, and request maximum. By adjusting these values you can configure a general policy; for example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **request** options so that each connection stays open longer and more requests are processed for each connection.

Another example would be to configure a policy that minimizes the response time for new connections. You can do this by specifying small values for the **life** and **request** options so that the connections are quickly released to serve new clients.

A throughput policy would be better for HTTP sessions with dedicated management applications, as it would allow the application to send more requests before the connection is closed, while a response time policy would be better for interactive HTTP sessions, as it would allow more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Access security policies for the HTTP server are configured using the **ip http authentication** command, which allows only selective users to access the server, and the **ip http access-class** command, which allows only selective IP hosts to access the server.

How to Configure the HTTP 1.1 Web Server

To enable the HTTP server and configure optional server characteristics, perform the following steps. The HTTP server is disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http authentication** (optional)
5. **ip http port** (optional)
6. **ip http path** (optional)
7. **ip http access-class** (optional)
8. **ip http max-connections** (optional)
9. **ip http timeout-policy** (optional)

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 server Example: Router(config)# ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface. Note If you are enabling the secure HTTP (HTTPS) server using the ip http secure-server command, you should disable the standard HTTP server using the no ip http server command. This is required to ensure only secure connections to the server.

	Command or Action	Purpose
Step 4	<pre>ip http authentication {aaa {command-authorization level listname exec-authorization listname login-authentication listname} enable local tacacs}</pre> <p>Example: Router(config)# ip http authentication aaa exec-authorization LOCALDB</p>	<p>(Optional) Specifies the authentication method to be used for login when a client connects to the HTTP server. The methods for authentication are:</p> <p>aaa—Indicates that the authentication method used for the AAA login service (specified by the aaa authentication login default command) should be used for authentication.</p> <p>enable—Indicates that the “enable” password should be used for authentication. (This is the default method.)</p> <p>local —Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.</p> <p>tacacs—Indicates that the TACACS (or XTACACS) server should be used for authentication.</p>
Step 5	<pre>ip http port port-number</pre> <p>Example: Router(config)# ip http port 8080</p>	<p>(Optional) Specifies the server port that should be used for HTTP communication (for example, for the Cisco Web browser user interface).</p>
Step 6	<pre>ip http path URL</pre> <p>Example: Router(config)# ip http path slot1:</p>	<p>(Optional) Sets the base HTTP path for HTML files. The base path is used to specify the location of the HTTP server files (HTML files) on the local system. Generally, the HTML files are located in system Flash memory.</p>
Step 7	<pre>ip http access-class access-list-number</pre> <p>Example: Router(config)# ip http access-class 20</p>	<p>(Optional) Specifies the access list that should be used to allow access to the HTTP server.</p>

Command or Action	Purpose
<p>Step 8</p> <pre>ip http max-connections value</pre> <p>Example: Router(config)# ip http max-connections 10</p>	<p>(Optional) Sets the maximum number of concurrent connections to the HTTP sever that will be allowed. The default value is 5.</p>
<p>Step 9</p> <pre>ip http timeout-policy idle seconds life seconds requests value</pre> <p>Example: Router(config)# ip http timeout-policy idle 30 life 120 requests 100</p>	<p>(Optional) Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are:</p> <p>idle—The maximum number of seconds the connection will be kept open if no data is received or response data can not be sent out on the connection. Note that a new value may not take effect on any already existing connections. If the server is too busy or the limit on the life time or the number of requests is reached, the connection may be closed sooner. The default value is 180 seconds (3 minutes).</p> <p>life—The maximum number of seconds the connection will be kept open, from the time the connection is established. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the number of requests is reached, it may close the connection sooner. Also, since the server will not close the connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes. The default value is 180 seconds (3 minutes). The maximum value is 86400 seconds (24 hours).</p> <p>requests—The maximum limit on the number of requests processed on a persistent connection before it is closed. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the life time is reached, the connection may be closed before the maximum number of requests are processed. The default value is 1. The maximum value is 86400.</p>

How to Configure the HTTP Client

The standard HTTP 1.1 client and the secure HTTP client are always enabled. No commands exist to disable the HTTP client. For information about configuring optional characteristics for the secure HTTP (HTTPS) client, see the “HTTPS - HTTP Server and Client with SSL 3.0” 12.2(15)T feature guide document.

To configure optional characteristics of the HTTP client, use any of the following optional commands.

1. **ip http client cache**
2. **ip http client connection**
3. **ip http client password**
4. **ip http client proxy-server**

5. ip http client response
6. ip http client source-interface
7. ip http client username

```
Router(config)#ip http client ?
cache                HTTP client cache
connection           Configure HTTP Client connection
password             Specify password for HTTP(S) file system client connections
proxy-server        Specify proxy server name for HTTP file system client
                    connections
response            How long HTTP Client waits for a response from the server
                    for a request message before giving up
source-interface     Specify interface for source address in all HTTP(S) client
                    connections
username            Specify username for HTTP(S) file system client connections
```

DETAILED STEPS

Command or Action	Purpose
<p>Step 1</p> <pre>ip http client cache ager interval <0-60> ip http client cache memory {file <kilobytes> pool <kilobytes> }</pre>	<pre>C3660-1(config)#ip http client cache ? ager Cache Ager Interval Time memory Maximum memory allowed for HTTP Client Cache C3660-1(config)#ip http client cache ager ? interval Interval Time C3660-1(config)#ip http client cache ager interval ? <0-60> Interval in Minutes<0-60>, default is 5 C3660-1(config)#ip http client cache ager interval 5 ? <cr> C3660-1(config)#ip http client cache memory ? file maximum file size allowed for caching pool maximum memory pool allowed for http cache C3660-1(config)#ip http client cache memory file ? <1-10> size of cache memory file in kbytes<1-10>, default is 2 C3660-1(config)#ip http client cache memory file 2 ? <cr> C3660-1(config)#ip http client cache memory pool ? <0-100> size of cache memory pool in kbytes <0-100>, default is 100 C3660-1(config)#ip http client cache memory pool 100 ? <cr> C3660-1(config)#ip http client cache ? ager Cache Ager Interval Time memory Maximum memory allowed for HTTP Client Cache</pre> <p>•</p>
<p>Step 2</p> <pre>ip http client connection {retry <1-5> idle timeout <1-60> persistent timeout <1-60>}</pre>	
<p>Step 3</p> <pre>ip http server</pre> <p>Example: Router(config)# ip http server</p>	<p>Enables the HTTP 1.1 server, including the Cisco web browser user interface.</p> <p>Note If you are enabling the secure HTTP (HTTPS) server using the ip http secure-server command, you should disable the standard HTTP server using the no ip http server command. This is required to ensure only secure connections to the server.</p>

	Command or Action	Purpose
Step 4	<pre>ip http authentication {aaa {command-authorization level listname exec-authorization listname login-authentication listname} enable local tacacs}</pre> <p>Example: Router(config)# ip http authentication aaa exec-authorization LOCALDB</p>	<p>(Optional) Specifies the authentication method to be used for login when a client connects to the HTTP server. The methods for authentication are:</p> <p>aaa—Indicates that the authentication method used for the AAA login service (specified by by the aaa authentication login default command) should be used for authentication.</p> <p>enable—Indicates that the “enable” password should be used for authentication. (This is the default method.)</p> <p>local —Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.</p> <p>tacacs—Indicates that the TACACS (or XTACACS) server should be used for authentication.</p>
Step 5	<pre>ip http port port-number</pre> <p>Example: Router(config)# ip http port 8080</p>	<p>(Optional) Specifies the server port that should be used for HTTP communication (for example, for the Cisco Web browser user interface).</p>
Step 6	<pre>ip http path URL</pre> <p>Example: Router(config)# ip http path slot1:</p>	<p>(Optional) Sets the base HTTP path for HTML files. The base path is used to specify the location of the HTTP server files (HTML files) on the local system. Generally, the HTML files are located in system Flash memory.</p>
Step 7	<pre>ip http access-class access-list-number</pre> <p>Example: Router(config)# ip http access-class 20</p>	<p>(Optional) Specifies the access list that should be used to allow access to the HTTP server.</p>

Command or Action	Purpose
<p>Step 8</p> <pre>ip http max-connections value</pre> <p>Example: Router(config)# ip http max-connections 10</p>	<p>(Optional) Sets the maximum number of concurrent connections to the HTTP sever that will be allowed. The default value is 5.</p>
<p>Step 9</p> <pre>ip http timeout-policy idle seconds life seconds requests value</pre> <p>Example: Router(config)# ip http timeout-policy idle 30 life 120 requests 100</p>	<p>(Optional) Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are:</p> <p>idle—The maximum number of seconds the connection will be kept open if no data is received or response data can not be sent out on the connection. Note that a new value may not take effect on any already existing connections. If the server is too busy or the limit on the life time or the number of requests is reached, the connection may be closed sooner. The default value is 180 seconds (3 minutes).</p> <p>life—The maximum number of seconds the connection will be kept open, from the time the connection is established. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the number of requests is reached, it may close the connection sooner. Also, since the server will not close the connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes. The default value is 180 seconds (3 minutes). The maximum value is 86400 seconds (24 hours).</p> <p>requests—The maximum limit on the number of requests processed on a persistent connection before it is closed. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the life time is reached, the connection may be closed before the maximum number of requests are processed. The default value is 1. The maximum value is 86400.</p>

Configuration Examples for the HTTP 1.1 Web Server

The following example shows a typical configuration that enables the server and sets some of the characteristics:

```
Router(config)# ip http server
Router(config)# ip http authentication aaa exec-authorization LOCALDB
Router(config)# ip http path flash:
Router(config)# ip http access-class 10
Router(config)# ip http max-connections 10
```

In the following example, a Throughput timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will remain open (be “alive”) until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Verifying HTTP Connectivity

To verify remote connectivity to the HTTP server, enter the system IP address in a Web browser, followed by a colon and the appropriate port number (80 is the default port number).

For example, if the system IP address is 209.165.202.128 and the port number is 8080, enter **http://209.165.202.128:8080** as the URL in a Web browser.

If HTTP authentication is configured, a login dialog box will appear. Enter the appropriate user name and password. If the default login authentication method of “enable” is configured, you may leave the username field blank, and use the “enable” password to log in.

The system home page should appear in your browser.

Where to Go Next

For information about secure HTTP connections using Secure Socket Layer (SSL) 3.0, refer to the “HTTPS - HTTP with SSL 3.0” 12.2(15)T feature document listed below.

Additional References

For additional information related to the HTTP 1.1 Web Server and Client, refer to the following references:

Related Documents

Related Topic	Document Title
HTTPS	“HTTPS - HTTP with SSL 3.0,” 12.2(15)T feature document: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsslsh.htm
HTTPS	“Firewall Support of HTTPS Authentication Proxy,” 12.2(15)T feature document

Standards

No specific standards are supported by this feature. Note that HTTP 1.1, as defined in RFC 2616, is currently classified as a “Standards Track” document by the IETF.

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> No specific MIBs are supported for this feature. 	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

RFCs

RFCs ¹	Title
RFC 2616	“Hypertext Transfer Protocol -- HTTP/1.1”

1. Not all supported RFCs are listed.

The Cisco implementation of the HTTP version 1.1 supports a subset of elements defined in RFC 2616. The following is a list of supported RFC 2616 headers:

- Allow (Only GET, HEAD, and POST methods are supported)
- Authorization, WWW-Authenticate - Basic authentication only
- Cache-control
- Chunked Transfer Encoding
- Connection close
- Content-Encoding
- Content-Language
- Content-Length
- Content-Type
- Date, Expires
- Location

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 the commands used to configure the HTTP 1.1 Web Server and HTTP 1.1 Web Client. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

- [debug ip http all](#)
- [ip http access-class](#)
- [ip http max-connections](#)
- [ip http path](#)
- [ip http port](#)

- [ip http server](#)
- [ip http timeout-policy](#)
- [show ip http server](#)

debug ip http all

To enable debugging output for all HTTP processes on the system, use the **debug ip http all** command in privileged EXEC mode. To disable HTTP debugging output, use the **no** form of this command.

debug ip http all

no debug ip http all

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command enables debugging messages for all HTTP processes and activity. Issuing this command is equivalent to issuing the following commands:

- **debug ip http authentication**
- **debug ip http ezsetup**
- **debug ip http ssi**
- **debug ip http token**
- **debug ip http transaction**
- **debug ip http url**

Examples

For sample output and field descriptions of this command, see the documentation of the commands listed in the “Usage Guidelines” section.

Related Commands

Command	Description
debug ip http authentication	Displays authentication progress messages for the HTTP server.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http ssi	Displays Server Side Includes (SSI) translations and SSI ECHO command execution.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed on the router’s HTTP server from remote clients.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

ip http access-class *access-list-number*

no ip http access-class *access-list-number*

Syntax Description	<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list global configuration command.
---------------------------	---------------------------	--

Defaults	No access list is applied to the HTTP server.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.
-------------------------	--

Examples	In the following example the access list identified as “20” is defined and assigned to the HTTP server:
-----------------	---

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.0 0.0.0.255
Router(config-std-nacl)# permit 209.165.0.0 0.0.255.255
Router(config-std-nacl)# permit 209.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit
Router(config)# ip http access-class 20
```

Related Commands	Command	Description
	ip access-list	Assigns an ID to an access list and enters access list configuration mode.
	ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http max-connections

To configure the maximum number of concurrent connections allowed for the HTTP server, use the **ip http max-connections** command in global configuration mode. To return the maximum connection value to the default, use the **no** form of this command.

ip http max-connections *value*

no ip http max-connections *value*

Syntax Description	<i>value</i>	The maximum number of concurrent HTTP connections. The range is 1 to 16. The default is 5.
---------------------------	--------------	--

Defaults 5 concurrent HTTP connections.

Command Modes Global configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines Platform-specific implementations can supercede the upper range limit of 16.

If a new value is configured that is less than the previously configured value while the current number of connections exceeds the new maximum value, the HTTP server will not abort any of the current connections. However, the server will not accept any new connections until the current number of connections falls below the new configured value.

Examples In the following example the HTTP server is configured to allow up to 10 simultaneous connections:

```
Router(config)# ip http server
Router(config)# ip http max-connections 10
```

Related Commands	Command	Description
		ip http server

ip http path

To specify the base path used to locate files for use by the HTTP server, use the **ip http path** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http path *URL*

no ip http path *URL*

Syntax Description	<i>URL</i>	Cisco IOS File System (IFS) Uniform Resource Locator (URL) specifying the location of the HTML files used by the HTTP server.
---------------------------	------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	<p>After enabling the HTTP server, you should set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP Web Server typically reside in system Flash memory. Remote URLs can be specified using this command, but use of remote pathnames (for example, where HTML files are located on a remote TFTP server) is not recommended.</p>
-------------------------	---

Examples	<p>In the following example, the HTML files are located in the default Flash location on the system:</p> <pre>Router(config)# ip http path flash:</pre> <p>In the following example, the HTML files are located in the directory named “web” on the Flash memory card inserted in slot 0:</p> <pre>Router(config)# ip http path slot0:web</pre>
-----------------	---

Related Commands	Command	Description
	ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http port

To specify the port number to be used by the HTTP server, use the **ip http port** command in global configuration mode. To return the port number to the default, use the **no** form of this command.

ip http port *port-number*

no ip http port *port-number*

Syntax Description

<i>port-number</i>	The port number to be used for the HTTP server. Valid values are 80 or any value from 1024 to 65535. The default is 80.
--------------------	---

Defaults

The HTTP server uses port 80.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	This command was modified to restrict port numbers. The port number 443 is now reserved for HTTPS (HTTP over SSL) connections.

Usage Guidelines

HTTP port 80 is the standard port used by web servers.

Examples

In the following example the HTTP server port is changed to port 8080.

```
Router(config)# ip http server
Router(config)# ip http port 8080
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http server

To enable the HTTP server on your system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Defaults

The HTTP server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation.

Usage Guidelines

The HTTP server uses the standard port 80 by default.



Caution

The standard HTTP server and the secure HTTP server can run at the same time on your system. If you enable the secure HTTP server using the **ip http secure-server** command, you should disable the standard HTTP server using the **no ip http server** command to ensure that secure data can not be accessed through the standard HTTP connection.

Examples

In the following example the HTTP server is enabled:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http path	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http timeout-policy

To configure the parameters for closing connections to the local HTTP server, use the **ip http timeout-policy** command in global configuration mode. To return the parameters to their defaults, use the **no** form of this command.

ip http timeout-policy idle *seconds* **life** *seconds* **requests** *value*

no ip http timeout-policy

Syntax Description

idle <i>seconds</i>	The maximum number of seconds the connection will be kept open if no data is received or response data can not be sent out on the connection. The valid range is from 1 to 600 seconds (10 minutes). The default value is 180 seconds (3 minutes).
life <i>seconds</i>	The maximum number of seconds the connection will be kept open, from the time the connection is established. The valid range is from 1 to 86400 seconds (24 hours). The default value is 180 seconds (3 minutes).
requests <i>value</i>	The maximum limit on the number of requests processed on a persistent connection before it is closed. The valid range is from 1 to 86400. The default value is 1.

Defaults

HTTP server connection idle time: 180 seconds (3 minutes)
 HTTP server connection life time: 180 seconds (3 minutes)
 HTTP server connection maximum requests: 1

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command sets the characteristics that determine how long a connection to the HTTP server should remain open.

This command may not take effect immediately on any HTTP connections that are open at the time you use this command. In other words, new values for idle time, life time, and maximum requests will apply only to connections made to the HTTP server after this command is issued.

A connection may be closed sooner than the configured **idle** time if the server is too busy or the limit on the **life** time or the number of **requests** is reached.

A connection may be closed sooner than the configured **life** time if the server is too busy or the limit on the **idle** time or the number of **requests** is reached. Also, since the server will not close a connection while actively processing a request, the connection may remain open longer than the specified **life** time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes.

A connection may be closed before the maximum number of requests are processed if the server is too busy or the limit on the **idle** time or **life** time is reached.

The **ip http timeout-policy** command allows you to specify a general access policy to the HTTP server by adjusting the connection timeout values. For example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **request** options so that each connection stays open longer and more requests are processed for each connection.

Another example would be to configure a policy that minimizes the response time for new connections. You can do this by specifying small values for the **life** and **request** options so that the connections are quickly released to serve new clients.

A throughput policy would be better for HTTP sessions with dedicated management applications, as it would allow the application to send more requests before the connection is closed, while a response time policy would be better for interactive HTTP sessions, as it would allow more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Examples

In the following example, a Throughput timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will remain open (be “alive”) until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in 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 Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

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

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
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 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 can not 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.

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

Field	Description
HTTP Secure Server Capability:	Indicates if the running software image supports the secure HTTP server (“Present” or “Not Present”). If the capability is present, the output from the show ip http secure-server status command will appear after this line.
HTTP server application session modules:	Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including: <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:	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: <i>hh:mm:ss month/day</i>

The following example shows sample output for 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-edc-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, the output will end with the following line:

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

The following example shows sample output for the **show ip http server status** command when the software image does not support SSL (and, by extension, does not support the secure HTTP server):

```
Router> show ip http server status
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: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Not present
```

Related Commands

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

This document applies to Cisco IOS Release 12.2(15)T and derivative releases.

This document first published March 13th, 2003. Last updated June 16, 2003.

