



HTTP Services Configuration Guide, Cisco IOS Release 12.2SX

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

HTTP 1.1 Web Server and Client	1
Finding Feature Information	1
Information About the HTTP 1.1 Web Server and Client	1
About HTTP Server General Access Policies	2
How to Configure HTTP 1.1 Web Server and Client	2
Configuring the HTTP 1.1 Web Server	3
Configuring the HTTP Client	5
Configuration Examples for HTTP 1.1 Web Server	7
Configuring the HTTP 1.1 Web Server Example	7
Verifying HTTP Connectivity	8
Where to Go Next	8
Additional References	8
Feature Information for the HTTP 1.1 Web Server and Client	10



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. When combined with the HTTPS feature, the HTTP 1.1 Web Server and Client feature provides a complete, secure solution for HTTP services between Cisco devices.

This module describes the concepts and the tasks related to configuring the HTTP 1.1 Web Server and Client feature.

- [Finding Feature Information, page 1](#)
- [Information About the HTTP 1.1 Web Server and Client, page 1](#)
- [How to Configure HTTP 1.1 Web Server and Client, page 2](#)
- [Configuration Examples for HTTP 1.1 Web Server, page 7](#)
- [Where to Go Next, page 8](#)
- [Additional References, page 8](#)
- [Feature Information for the HTTP 1.1 Web Server and Client, page 10](#)

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 Table at the end of this document.

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. An account on Cisco.com is not required.

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 (SSIs) 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:

- Cisco web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server
- VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM)
- QoS Device Manager (QDM) application, which uses the QDM Server
- IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS)

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

- [About HTTP Server General Access Policies, page 2](#)

About HTTP Server General Access Policies

The **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 configure this type of policy 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 configure this type of policy 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, the **ip http access-class** command, which allows only selective IP hosts to access the server, and the **ip http accounting commands** command, which specifies a particular command accounting method for HTTP server users.

How to Configure HTTP 1.1 Web Server and Client

- [Configuring the HTTP 1.1 Web Server, page 3](#)
- [Configuring the HTTP Client, page 5](#)

Configuring the HTTP 1.1 Web Server

Perform this task to enable the HTTP server and configure optional server characteristics. The HTTP server is disabled by default.



Note

If you want to configure authentication (step 4), you must configure the authentication type before you begin configuring the HTTP 1.1 web server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http authentication** {aaa | enable | local | tacacs}
5. **ip http accounting commands level** {default | named-accounting-method-list}
6. **ip http port** port-number
7. **ip http path** url
8. **ip http access-class** access-list-number
9. **ip http max-connections** value
10. **ip http timeout-policy idle** seconds **life** seconds **requests** value

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>ip http server</p> <p>Example:</p> <pre>Router(config)# ip http server</pre>	<p>Enables the HTTP 1.1 server, including the Cisco web browser user interface.</p> <p>Note If you are enabling the HTTP over Secure Socket Layer (HTTPS) server using the ip http secure-server command, you should disable the standard HTTP server using the no ip http server command. This command is required to ensure only secure connections to the server.</p>

Command or Action	Purpose
<p>Step 4 <code>ip http authentication {aaa enable local tacacs}</code></p> <p>Example:</p> <pre>Router(config)# ip http authentication local</pre>	<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> <ul style="list-style-type: none"> • 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. • enable --Indicates that the “enable” password should be used for authentication. (This is the default method.) • 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. • tacacs --Indicates that the TACACS (or XTACACS) server should be used for authentication.
<p>Step 5 <code>ip http accounting commands level {default named-accounting-method-list}</code></p> <p>Example:</p> <pre>Router(config)# ip http accounting commands 15 default</pre>	<p>(Optional) Specifies a particular command accounting method for HTTP server users.</p> <ul style="list-style-type: none"> • Command accounting for HTTP and HTTPS is automatically enabled when authentication, authorization, and accounting (AAA) is configured on the device. It is not possible to disable accounting for HTTP and HTTPS. HTTP and HTTPS will default to using the global AAA default method list for accounting. The CLI can be used to configure HTTP and HTTPS to use any predefined AAA method list. • <i>level</i> --Valid privilege level entries are integers from 0 to 15. • default --Indicates the default accounting method list configured by the aaa accounting commands CLI. • <i>named-accounting-method-list</i> --Indicates the name of the predefined command accounting method list.
<p>Step 6 <code>ip http port port-number</code></p> <p>Example:</p> <pre>Router(config)# ip http port 8080</pre>	<p>(Optional) Specifies the server port that should be used for HTTP communication (for example, for the Cisco web browser user interface).</p>
<p>Step 7 <code>ip http path url</code></p> <p>Example:</p> <pre>Router(config)# ip http path slot1:</pre>	<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>

Command or Action	Purpose
<p>Step 8 <code>ip http access-class <i>access-list-number</i></code></p> <p>Example:</p> <pre>Router(config)# ip http access-class 20</pre>	<p>(Optional) Specifies the access list that should be used to allow access to the HTTP server.</p>
<p>Step 9 <code>ip http max-connections <i>value</i></code></p> <p>Example:</p> <pre>Router(config)# ip http max- connections 10</pre>	<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 10 <code>ip http timeout-policy <i>idle seconds life seconds requests value</i></code></p> <p>Example:</p> <pre>Router(config)# ip http timeout-policy idle 30 life 120 requests 100</pre>	<p>(Optional) Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are:</p> <ul style="list-style-type: none"> • idle --The maximum number of seconds the connection will be kept open if no data is received or response data cannot 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). • 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). • 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 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.

Configuring the HTTP Client

Perform this task to enable the HTTP client and configure optional client characteristics.

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 HTTPS client, see the *HTTPS-HTTP Server and Client with SSL 3.0*, Release 12.2(15)T, feature module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http client cache {ager interval *minutes* | memory {file *file-size-limit* | pool *pool-size-limit*}**
4. **ip http client connection {forceclose | idle timeout *seconds* | retry count | timeout *seconds*}**
5. **ip http client password *password***
6. **ip http client proxy-server *proxy-name* proxy-port *port-number***
7. **ip http client response timeout *seconds***
8. **ip http client source-interface *type number***
9. **ip http client username *username***

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 client cache {ager interval <i>minutes</i> memory {file <i>file-size-limit</i> pool <i>pool-size-limit</i>} Example: Router(config)# ip http client cache memory file 5	Configures HTTP client cache.
Step 4 ip http client connection {forceclose idle timeout <i>seconds</i> retry count timeout <i>seconds</i>} Example: Router(config)# ip http client connection timeout 10	Configures an HTTP client connection.
Step 5 ip http client password <i>password</i> Example: Router(config)# ip http client password pswd1	Configures the default password used for connections to remote HTTP servers.

Command or Action	Purpose
<p>Step 6 <code>ip http client proxy-server <i>proxy-name</i> proxy-port <i>port-number</i></code></p> <p>Example:</p> <pre>Router(config)# ip http client proxy-server server1 proxy-port 52</pre>	Configures an HTTP proxy server.
<p>Step 7 <code>ip http client response timeout <i>seconds</i></code></p> <p>Example:</p> <pre>Router(config)# ip http client response timeout 60</pre>	Specifies the timeout value, in seconds, that the HTTP client waits for a response from the server.
<p>Step 8 <code>ip http client source-interface <i>type number</i></code></p> <p>Example:</p> <pre>Router(config)# ip http client source-interface ethernet1/0</pre>	Configures a source interface for the HTTP client.
<p>Step 9 <code>ip http client username <i>username</i></code></p> <p>Example:</p> <pre>Router(config)# ip http client user1</pre>	Configures the default username used for connections to remote HTTP servers.

Configuration Examples for HTTP 1.1 Web Server

- [Configuring the HTTP 1.1 Web Server Example, page 7](#)
- [Verifying HTTP Connectivity, page 8](#)

Configuring the HTTP 1.1 Web Server Example

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

```
ip http server
ip http authentication aaa
ip http accounting commands 15 default
ip http path flash:
ip access-list standard 20
  permit 209.165.202.130 0.0.0.255
  permit 209.165.201.1 0.0.255.255
  permit 209.165.200.225 0.255.255.255
! (Note: all other access implicitly denied)
end
ip http access-class 10
ip http max-connections 10
ip http accounting commands 1 oneacct
```

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.

```
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.

```
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 209.165.202.129 and the port number is 8080, enter `http://209.165.202.129:8080` as the URL in a web browser.

If HTTP authentication is configured, a login dialog box will appear. Enter the appropriate username 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 Sockets Layer (SSL) 3.0, refer to the *HTTPS - HTTP with SSL 3.0*, Release 12.2(15)T, feature module at: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftsslsh.html

Additional References

The following sections provide references related to the HTTP 1.1 Web Server and Client.

Related Documents

Related Topic	Document Title
HTTPS	<ul style="list-style-type: none"> HTTPS--HTTP with SSL 3.0 feature module Firewall Support of HTTPS Authentication Proxy feature module
HTTP commands	<i>Cisco IOS Network Management Command Reference</i>

Standards

Standard	Title
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

MIB	MIBs Link
<ul style="list-style-type: none"> No specific MIBs are supported for this feature. 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC ¹	Title
RFC 2616	<i>Hypertext Transfer Protocol -- HTTP/1.1</i>

The Cisco implementation of the HTTP version 1.1 supports a subset of elements defined in RFC 2616. 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

¹ Not all supported RFCs are listed.

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

Feature Information for the HTTP 1.1 Web Server and Client

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. An account on Cisco.com is not required.

Table 1 **Feature Information for HTTP 1.1 Web Server and Client**

Feature Name	Releases	Feature Information
HTTP 1.1 Web Server and Client	12.2(15)T 12.2(33)SB 12.2(33)SRC 12.4(15)T Cisco IOS XE 3.1.0SG	<p>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. When combined with the HTTPS feature, the HTTP 1.1 Web Server and Client feature provides a complete, secure solution for HTTP services between Cisco devices.</p> <p>The following commands were introduced or modified by this feature: debug ip http all, debug ip http client, ip http access-class, ip http authentication, ip http client cache, ip http client connection, ip http client password, ip http client proxy-server, ip http client response timeout, ip http client source-interface, ip http client username, ip http max-connections, ip http path, ip http port, ip http server, ip http timeout-policy, show ip http client, show ip http client connection, show ip http client history, show ip http client session-module, show ip http server, show ip http server secure status.</p>

Feature Name	Releases	Feature Information
HTTP TACAC+ Accounting Support	12.2(33)SB 12.2(33)SRC 12.2(50)SY 12.4(15)T	<p>The HTTP TACAC+ Accounting Support feature introduces the ip http accounting commands command. This command is used to specify a particular command accounting method for HTTP server users. Command accounting provides information about the commands for a specified privilege level that are being executed on a device. Each command accounting record corresponds to one IOS command executed at its respective privilege level, as well as the date and time the command was executed, and the user who executed it. The following sections provide information about this feature:</p> <p>The following commands were introduced or modified by this feature: ip http accounting commands.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

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.