



Cisco IOS HTTP Server, Client and Web Browser User Interface Commands

This chapter provides descriptions of the commands used to enable the HTTP server and secure HTTP server on your router. The HTTP server allows the use of the Cisco IOS Web browser user interface (UI) and additional services, such as ClickStart.

For configuration tasks and examples, refer to the “Using the Cisco Web Browser User Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*.

international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]), use the **international** command in line configuration mode. To display characters in 7-bit format, use the **no** form of this command.

international

no international

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines If you are configuring a Cisco IOS platform using the Cisco Web browser UI, this feature is enabled automatically when you enable the Cisco Web browser UI using the **ip http server** global configuration command.

Examples The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) when you are using Telnet to access the platform:

```
line vty 4
  international
```

Related Commands	Command	Description
	terminal international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[]) for a current Telnet session in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).

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 authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication {aaa | enable | local | tacacs}

no ip http authentication {aaa | enable | local | tacacs}

Syntax Description		
aaa	Indicates that the authentication method used for the AAA login service should be used for authentication. The AAA login service method is specified by the aaa authentication login default command.	
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.	

Defaults The “enable” password is required when users (clients) connect to the HTTP server.

Command Modes Global configuration

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server.

If the enable password is used, the client connects to the HTTP server with a default privilege level of 15.

Use of the **ip http authentication aaa** command is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

Examples The following example specifies that the method configured for AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “enable” password method.

```
Router(config)# ip http authentication aaa
Router(config)# aaa authentication login default enable
```

Related Commands	Command	Description
	ip http server	Enables the HTTP server.
	aaa authentication login	Specifies the login authentication method to be used by the authentication, authorization, and accounting (AAA) service.

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

```
ip http client secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5]
[des-cbc-sha]}
```

```
no ip http client secure-ciphersuite
```

Syntax Description		
	3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.
	rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
	rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and MD5 for message digest.
	des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Defaults

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuite(s) to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

In the following example the HTTPS client is configured to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

Related Commands

Command	Description
show ip http client secure status	Displays the configuration status of the secure HTTP client.

ip http client secure-trustpoint

To specify the remote CA trustpoint that should be used if certification is needed for the secure HTTP client, use the **ip http client secure-trustpoint** command in global configuration mode. To remove a client trustpoint from the configuration, use the **no** form of this command.

ip http client secure-trustpoint *trustpoint-name*

no ip http client secure-trustpoint *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated crypto ca trustpoint command.
------------------------	--

Defaults

If the remote HTTPS server requests client certification, the secure HTTP client will use the trustpoint configured as **primary** in the CA trustpoint configuration.

If a trustpoint is not configured, client certification will fail.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used by the secure HTTP (HTTPS) client for cases when the remote HTTPS server requires client authorization.

Use of this command assumes you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated sub-mode commands. If the remote HTTPS server requires client authorization and a trustpoint is not configured for the client, the remote HTTPS server will reject the connection.

If this command is not used, the client will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** CA TrustPoint configuration mode command.

Examples

In the following example the CA trustpoint is configured then referenced in the secure HTTP server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
!The following command is used to actually obtain the security certificate.
```

```
!A trustpoint NAME is used because there could be multiple trust points
!configured for the router.
Router(config)# crypto ca enrollment TP1
!The following command specifies that the secure HTTP client
!should use the certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http client secure-trustpoint tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Specifies a name for a certificate authority trustpoint and enters CA TrustPoint configuration mode.
primary	Indicates that the CA trustpoint being configured should be used as the primary (default) trustpoint.

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	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

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
	12.0	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 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 secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

```
ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]}
```

```
no ip http secure-ciphersuite
```

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and MD5 for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Defaults

The HTTPS server negotiates the best CipherSuite using the list received from connecting client.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuite(s) to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites) :

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5

3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Socket Layer (SSL) 3.0 protocol.

Examples

The following example restricts the CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

Related Commands

Command	Description
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-client-auth

To configure the secure HTTP sever to authenticate connecting clients, use the **ip http secure-client-auth** command in global configuration mode. To remove the requirement for client authorization, use the **no** form of this command.

ip http secure-client-auth

no ip http secure-client-auth

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled (that is, client authentication is not required for connections to the secure HTTP server).

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.

In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.

Examples

In the following example the secure web server is enabled and the server is configured to accept connections only from clients with a signed security certificate:

```
Router(config)# no ip http server
Router(config)# ip http secure-server
Router(config)# ip http secure-client-auth
```

Related Commands

Command	Description
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-port

To specify the port (socket) to be used for connections to the secure HTTP (HTTPS) sever, use the **ip http secure-port** command in global configuration mode. To return the secure HTTP server port number to the default, use the **no** form of this command.

ip http secure-port *port-number*

no ip http secure-port

Syntax Description	<i>port-number</i>	Port number that should be used for the secure HTTP server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.
---------------------------	--------------------	---

Defaults	Port 443
-----------------	----------

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

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

Examples

The following example changes the port for HTTPS server connections from 443 to 1025:

```
Router(config)# ip http secure-port 1025
```

Related Commands	Command	Description
	ip http secure-server	Enables the secure HTTP (HTTPS) server.

ip http secure-server

To enable the secure HTTP web server, use the **ip http secure-server** command in global configuration mode. To disable the secure HTTP server, use the **no** form of this command.

ip http secure-server

no ip http secure-server

Syntax Description This command has no arguments or keywords.

Defaults The secure HTTP server is disabled.

Command Modes Global configuration

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

Usage Guidelines The secure HTTP server (also called the HTTPS server) uses the Secure Socket Layer (SSL) version 3.0 protocol.



Note

When enabling the secure HTTP server you should always disable the standard HTTP server to prevent insecure connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this is a precautionary step; typically, the HTTP server is disabled by default).

If a certificate authority is to be used for certification, you should declare the CA trustpoint on the routing device before enabling the secure HTTP server.

Examples In the following example the secure HTTP server is enabled, and the (previously configured) CA trustpoint CA_trust_local is specified:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http secure-server
Router(config)# ip http secure-trustpoint CA_trust_local
Router(config)# end
Router# show ip http server secure status
HTTP secure server status: Enabled
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: CA_trust_local
```

■ ip http secure-server

Related Commands	Command	Description
	ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the secure HTTP server.
	show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-trustpoint

To specify the certificate authority (CA) trustpoint that should be used for obtaining signed certificates for the secure HTTP server, use the **ip http secure-trustpoint** command in global configuration mode. To remove a previously specified CA trustpoint, use the **no** form of this command.

ip http secure-trustpoint *trustpoint-name*

no ip http secure-trustpoint *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated crypto ca trustpoint command.
------------------------	--

Defaults

The secure HTTP server will use the trustpoint configured as **primary** in the CA trustpoint configuration.

If a trustpoint is not configured, the secure HTTP server will use a self-signed certificate.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command specifies that the secure HTTP server should use the X.509v3 certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used to authenticate the server to connecting clients, and, if remote client authentication is enabled, to authenticate the connecting clients.

Use of this command assumes you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated sub-mode commands. If a trustpoint is not configured, the secure HTTP server will use a self-signed certificate.

If this command is not used, the server will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** CA TrustPoint configuration mode command.

Examples

In the following example the CA trustpoint is configured, a certificate is obtained, then the certificate is referenced in the secure HTTP server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
!A trustpoint NAME is used because there could be multiple trustpoints
!configured for the router.
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
```

ip http secure-trustpoint

```

Router(config-ca)# exit
Router(config)# crypto ca authenticate tp1
!The following command is used to actually obtain the security certificate.
Router(config)# crypto ca enrollment tp1
Router(config)# ip http secure-server
!The following command specifies that the secure HTTP server
!should use a certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http secure-trustpoint tp1

```

Related Commands

Command	Description
crypto ca trustpoint	Declares the certificate authority (CA) that your routing device should use.
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

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. The secure HTTP server feature was added.

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	Specifies the base path used to locate files for use by the HTTP server.
	ip http secure-server	Enables the secure HTTP server.

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 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	
	User EXEC
	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.

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
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 16 describes the significant fields shown in the display.

Table 16 *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 16 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 server secure 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, only the following line will be visible:

```
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 secure HTTP (HTTPS) server.
show ip http server secure status	Displays the status of the secure HTTP (HTTPS) server.

terminal international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) for a current Telnet session, use the **terminal international** command in EXEC mode. To display characters in 7-bit format for a current Telnet session, use the **no** form of this command.

terminal international

no terminal international

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines If you are configuring a Cisco IOS platform using the Cisco Web browser UI, this feature is enabled automatically when you enable the Cisco Web browser UI using the **ip http server** global configuration command.

Examples The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) when you are using Telnet to access the platform for the current Telnet session:

```
Router# terminal international
```

Related Commands	Command	Description
	international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[]) in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).
