



Cisco IOS Web Browser Commands

This chapter provides detailed descriptions of the commands used to issue Cisco IOS commands from the Cisco Web browser accessible from the home page of your router.

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

international

If you are 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** line configuration command. Use the **no** form of this command to display characters in 7-bit format.

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 interface, this feature is enabled automatically when you enable the Cisco Web browser using the **ip http server** command.

Examples

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

```
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 assign an access list to the Hypertext Transfer Protocol server used by the Cisco IOS ClickStart software or the Cisco Web browser interface, use the **ip http access-class** global configuration command. To remove the assigned access list, use the **no** form of this command.

```
ip http access-class {access-list-number | name}
```

```
no ip http access-class {access-list-number | name}
```

Syntax Description	<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list (standard) command.
	<i>name</i>	Name of a standard IP access list, as configured by the ip access-list command.

Defaults There is no access list 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 The following example assigns the access list named marketing to the HTTP server:

```
ip http access-class marketing
ip access-list standard marketing
 permit 192.5.34.0 0.0.0.255
 permit 128.88.0.0 0.0.255.255
 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

Related Commands	Command	Description
	ip access-list	Defines an IP access list by name.
	ip http server	Enables monitoring or configuring of routers using the Cisco Web Browser interface.

ip http authentication

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

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

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

Syntax Description

aaa	Indicates that the AAA facility is used for authentication.
enable	Indicates that the "enable" password is used for logon authentication. This is the default.
local	Indicates that the local user database as defined on the Cisco router or access server is used for authentication.
tacacs	Indicates that the TACACS or XTACACS server is used for authentication.

Defaults

The default method of authentication for the HTTP server interface is the enable password method.

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

The "enable" password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.



Note

When the "enable" password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the "enable" password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only "enable" password for authentication is strongly discouraged. Instead, use of the **local** or **tacacs** authentication options, configured as part of a global Authentication, Authorization, and Accounting (AAA) framework, is recommended.

To configure HTTP access as part of a AAA policy, use the **ip http authentication aaa** command option. The "local", "tacacs", or "enable" authentication methods should then be configured using the **aaa authentication login** command.

For information about adding users into the local username database, refer to the [Cisco IOS Security Configuration Guide](#).

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 “local” username/password authentication method.

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

Related Commands

Command	Description
ip http server	Enables a Cisco 1003, Cisco 1004, or Cisco 1005 router to be configured from a browser using the Cisco IOS ClickStart software, and enables any router to be monitored or have its configuration modified from a browser using the Cisco Web browser interface.

ip http port

To specify the port to be used by the Cisco IOS ClickStart software or the Cisco Web browser interface, use the **ip http port** global configuration command. To use the default port, use the **no** form of this command.

ip http port *number*

no ip http port

Syntax Description	<i>number</i>	Port number for use by ClickStart or the Cisco Web browser interface.
--------------------	---------------	-----------------------------------------------------------------------

Defaults	80
----------	----

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	Use this command if ClickStart or the Cisco Web browser interface cannot use port 80.
------------------	---------------------------------------------------------------------------------------

Examples	The following example configures the router so that you can use ClickStart or the Cisco Web browser interface via port 60:
----------	----------------------------------------------------------------------------------------------------------------------------

```
ip http server
ip http port 60
```

Related Commands	Command	Description
	ip http server	Enables a Cisco 1003, Cisco 1004, or Cisco 1005 router to be configured from a browser using the Cisco IOS ClickStart software, and enables any router to be monitored or have its configuration modified from a browser using the Cisco Web browser interface.

ip http server

To enable the Cisco Web browser interface on a router or access server, use the **ip http server** global configuration command. To disable this feature, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is automatically enabled on Cisco 1003, Cisco 1004, and Cisco 1005 routers that have not yet been configured. For Cisco 1003, Cisco 1004, and Cisco 1005 routers that have already been configured, and for all other routers, this feature is disabled.

Command Modes

Global configuration

Usage Guidelines

The Cisco Web browser interface (which enables your router to perform as an HTTP server) allows configuration and monitoring of a router or access server using any web browser. Enabling the Cisco Web browser interface also allows Cisco 1003, Cisco 1004, and Cisco 1005 routers to be configured from a browser using the Cisco IOS Click Start software.

To view the home page of the router, use a Web browser pointed to `http://x.y.z.t`, where `x.y.z.t` is the IP address of your router or access server, or, if a name has been set, use `http://router-name`. Varying forms of authentication for login can be set using the **ip http authentication** command, but the default login method is entering the **enable** password when prompted.

For information on accessing a router Web page at a privilege level other than the default of 15 (privileged EXEC mode), see the “Using the Cisco Web Browser to Issue Commands” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example enables the Web (http) server on the router, allowing use of the Cisco Web browser interface to monitor the router and issue commands to it:

```
router(config)# ip http server
```

Related Commands	Command	Description
	ip http access-class	Assigns an access list to the HTTP server used by the Cisco IOS ClickStart software or the Cisco Web browser interface.
	ip http authentication	Specifies an authentication method for HTTP server users.
	ip http port	Specifies the port to be used by the Cisco IOS ClickStart software or the Cisco Web browser interface.

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** EXEC command. Use the **no** form of this command to display characters in 7-bit format for a current Telnet session.

terminal international

no terminal international

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes 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 interface, this feature is enabled automatically when you enable the Cisco Web browser using the **ip http server** 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:

```
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).
