Using the Cisco IOS Web Browser User Interface

The Cisco IOS software includes a Web browser user interface (UI) from which you can issue Cisco IOS commands. The Cisco IOS Web browser UI is accessed from the router home page, and can be customized for your business environment. For example, you can view pages in different languages and save them in Flash memory for easy retrieval.

For a complete description of the Cisco Web browser UI configuration commands in this chapter, refer to the "Cisco IOS Web Browser User Interface Commands"chapter of the *Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the *Cisco IOS Command Reference Master Index* or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Cisco IOS Web Browser User Interface

- You must have Cisco IOS Release 12.2 or a later release installed and running on your network
- To use the Cisco IOS Web browser UI, your computer must have a World Wide Web browser application.
- Most Cisco routers and access servers automatically generate a password protected home page when the HTTP server is enabled on the device. To access the home page, your computer must be on the same network as the router.

Restrictions for Cisco IOS Web Browser User Interface

- The Web browser UI is automatically enabled on the Cisco 1003, Cisco 1004, or Cisco 1005 routers to allow you to use ClickStart to configure your router. For all other Cisco devices, you must enable the Cisco Web browser UI.
- You can issue most Cisco IOS commands using a Web browser by connecting to the home page generated by the Cisco IOS software for your system.
- The Cisco Web browser UI works with most web browsers. Your Web browser must be able to read and submit forms.

Information About Cisco IOS Web Browser User Interface

Customizing the Cisco Web Browser UI

You can customize the HTML pages used by the Cisco Web browser UI to display Cisco IOS command output and Cisco IOS platform-specific variables (for example, a router host name or router address). You can display this information using HTML formatted Server Side Includes (SSIs) that you insert into your custom HTML pages.

Understanding SSIs

SSIs are HTML formatted commands or variables that you insert into HTML pages when you customize Cisco IOS platform configuration pages for a Web browser. These SSI commands and SSI variables display Cisco IOS command output and Cisco IOS platform-specific variables.

Note The majority of the customization features in this section are for the ClickStart EZsetup feature for the Cisco 1000 series, Cisco 1003/1004 series, and Cisco 1005 series routers only.

The Cisco IOS software supports two HTML SSI commands defined for customizing HTML pages: the SSI EXEC command and the SSI ECHO command. The HTML format of the SSI EXEC command is **<!--#execcmd="***xxx***"-->**, and the HTML format of the SSI ECHO command is **<!--#echovar="***yyy***"-->**. (See the section "Customizing HTML Pages Using SSIs" later in this chapter for a description of how to use these commands).

In addition to the two SSI commands, the Cisco IOS software supports several SSI variables defined for customizing HTML pages. SSI variables are used with the SSI ECHO command. One SSI variable is defined for all Cisco IOS platforms (SERVER_NAME), and other SSI variables are specifically defined for ISDN, Frame Relay, and asynchronous serial platforms. The format and a description of all the available SSI variables are provided in the table below. (See the section Customizing HTML Pages Using SSIs later in this chapter for a description of how to use these SSI variables with the SSI ECHO command).

The SSI EXEC command is supported on all platforms. The SSI ECHO command, used with SSI variables, is supported on all platforms listed in the table below.

Table 1: Description of SSI Variables

HTML Format of SSI Variable	Description of Variable Displayed on Browser Page	Cisco IOS Platforms This SSI Is Supported On
SERVER_NAME	Host name of the HTTP server.	All Cisco IOS platforms
EZSETUP_PASSWORD	Enable password (currently left blank).	Cisco 1000 series
EZSETUP_PASSWORD_VERIFY	Repeat of the enable password to verify accuracy (currently left blank).	Cisco 1000 series
EZSETUP_ETHERNET0_ADDRESS	IP address of the Ethernet interface 0.	Cisco 1000 series
EZSETUP_ETHERNET0_MASK	IP mask of the Ethernet interface 0.	Cisco 1000 series
EZSETUP_DNS_ADDRESS	Domain Name System (DNS) address used by the router.	Cisco 1000 series
EZSETUP_STANDARD_DEBUG_Y	Standard debug variable. Returns CHECKED if set to TRUE; otherwise, it is blank.	Cisco 1000 series
EZSETUP_STANDARD_DEBUG_N	Standard debug variable. Returns CHECKED if set to FALSE; otherwise, it is blank.	Cisco 1000 series
EZSETUP_ISDN_SWITCHTYPE	ISDN switch type.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_REMOTE_NAME	Name of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_REMOTE_NUMBER	Phone number of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_CHAP_PASSWORD	CHAP password of remote ISDN system.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPID1	ISDN SPID 1.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPID2	ISDN SPID 2.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPEED_56	Speed of ISDN interface. Returns CHECKED if set to 56K; otherwise, it is blank.	Cisco 1003 and Cisco 1004
EZSETUP_ISDN_SPEED_64	Speed of ISDN interface. Returns CHECKED if set to 64K; otherwise, it is blank.	Cisco 1003 and Cisco 1004
EZSETUP_FR_ADDRESS	Frame Relay IP address.	Cisco 1005
EZSETUP_FR_MASK	Frame Relay IP mask.	Cisco 1005
EZSETUP_FR_DLCI	Frame Relay DLCI.	Cisco 1005
EZSETUP_ASYNC_REMOTE_NAME	Name of remote system.	Cisco 1005
EZSETUP_ASYNC_REMOTE_NUMBER	Phone number of remote system.	Cisco 1005
EZSETUP_ASYNC_CHAP_PASSWORD	CHAP password for remote system.	Cisco 1005
EZSETUP_ASYNC_LINE_PASSWORD	Async line password.	Cisco 1005

HTML Format of SSI Variable	Description of Variable Displayed on Browser Page	Cisco IOS Platforms This SSI Is Supported On
EZSETUP_ASYNC_MODEM_SPEED	Speed of async modem (either 14.4K or 28.8K).	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_144K	Returns CHECKED if async modem speed is 14.4K; otherwise it is blank.	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_288K	Returns CHECKED if async modem speed is 28.8K; otherwise it is blank.	Cisco 1005

When you have designed a set of HTML pages that include SSIs, you can copy these pages to a Cisco IOS platform's Flash memory. When you retrieve these pages from Flash memory and display them using a Web browser, any SSI command that was designed into these pages will display either Cisco IOS command output or a current variable or identifier defined in the table below. For example, the SSI ECHO command with the variable SERVER_NAME will display the current host name of the HTTP server you are using, and the SSI ECHO command with the variable EZSETUP_ISDN_SWITCHTYPE will display the current ISDN switch type you are using.

Using SSIs, you can customize set of HTML pages to appear in languages other than English and copy these pages to Flash memory on multiple Cisco IOS platforms. When you retrieve these pages from the Flash memory of a Cisco IOS platform, current variables and identifiers associated with the platform you are currently using are displayed. SSIs save you from needing to duplicate these international pages (considered relatively large images that contain 8-bit or multibyte characters) and store them in the source code for each platform you are using.

Customizing HTML Pages Using SSIs

When you are customizing an HTML page for a Web browser, type **<!--#execcmd="***xxx***"-->** in your HTML file where you want Cisco IOS command output to appear on the browser page. Replace the *xxx variable* with any Cisco IOS EXEC mode command.

When you are customizing an HTML page for a Web browser, type **<!--#echovar="***yyy***"-->** in your HTML file where you want a value or identifier associated with a particular Cisco IOS platform (for example, an ISDN or Frame Relay platform) to appear on the browser page. Replace the *yyy* variable with an SSI variable described in the Description of SSI Variables table in the Understanding SSIs module.

Copying HTML Pages to Flash Memory

Once you have customized HTML pages using SSIs, copy your HTML pages to a Cisco IOS platform's Flash memory. To do this, save your pages using a filename appended with ".shtml" (for example, *filename* .shtml) and copy your file to Flash memory using a**copy** EXEC command (for example, the **copytftpflash** command). (Refer to the Cisco IOS command references for a **copy** command compatible with your platform.)

Displaying HTML Files Containing SSIs

When the Cisco Web browser UI is enabled, you can retrieve your HTML page from Flash memory and display it on the Cisco Web browser by typing **http://***router***/flash/***filename*in the URL window. Replace *router* with the host name or IP address of the current Cisco IOS platform you are using, and replace *filename* with the name of the file you created with ".shtml" appended, for example, http://myrouter/flash/ssi_file.shtml.

Methods of User Authentication

The **iphttpauthentication**command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **iphttpauthenticationaaa** command option is recommended. The**enable**, **local**, and **tacacs** methods should be specified using the **aaaauthenticationlogin** command.

If you do not use this command, the default authentication method is used. The default method of authentication for the HTTP server is to use the configured "enable" password. The "enable" password is configured with the **enablepassword** global configuration command. 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 **iphttpauthenticationaaa** command option. The "local", "tacacs", or "enable" authentication methods should then be configured using the **aaaauthenticationlogin** command.

For information about adding users into the local username database, refer to the Cisco IOS Security Configuration Guide.

Methods for Entering Commands

Entering Commands Using Hypertext Links

To enter a command using hypertext links, scroll through the commands listed at the bottom of the screen and click the one you want to execute. If the link is a complete command, it is executed. If the command has more parameters, another list of command hypertext links is displayed. Scroll through this second list and click the one you want to execute.

If the command is a request for information, like a **show** EXEC command, the information is displayed in the Web browser window.

If the command requires a variable, a form in which you can enter the variable is displayed.

Entering Commands Using the Command Field

Entering the command in the command field is just like entering it at a terminal console. Enter the command using the syntax documented in the Cisco IOS command reference. If you are uncertain of the options available for a particular command, type a question mark (**?**).

For example, entering **show?**in the command field displays the parameters for the **show**EXEC command. The Cisco Web browser UI displays the parameters as hypertext links. To select a parameter, you can either click on one of the links or you can enter the parameter in the command field.

Entering Commands Using the URL Window

You can issue a command using the URL window for the Web browser. To issue a command using the URL window, use the following syntax:

http:// *router-name* / [**level/***level/*]*command-mode/command*

The table below lists the URL arguments you must use when requesting a web page.

Table 2: Web Browser URL Argument Descriptions

Argument	Description
router-name	Name of the router being configured.
level/ *level*	(Optional) The privilege level you are requesting at which you are requesting access.
mode	The mode the command will be executed in, such as EXEC, configuration, or interface.
command	The command you want to execute. Replace spaces in the command syntax with forward slashes. If you do not specify a command in the URL, your browser will display a web page listing all of the commands available for the specified command mode.

For example, to execute a **showrunning-configuration** EXEC command on a router named example, you would enter the following in the URL window:

```
http://example/exec/show/running-configuration
```

After issuing this command, the Cisco Web browser UI will display the running configuration for the router.

The difference between entering a command in the Command field and entering a command in the URL window is that in the URL window, forward slashes should be used instead of spaces in the command syntax.

Specifying the Method for User Authentication

To specify how HTTP server users are authenticated, use the following command in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip http authentication** {**aaa**|**enable**	**local**	**tacacs**} **Example:** `Router(config)# ip http authentication tacacs`	Specifies how the HTTP server users are authenticated.

Example

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
```

Default Privilege Level

The default privilege level when accessing a router home page is privilege level 15 (global access). If privilege levels have been configured on the router and you have been assigned a privilege level other than 15, you must specify the privilege level to access the router home page.

When you specify a privilege level, the Cisco Web Browser UI will display and accept only those commands that have been defined for your user level. (For more information about privilege levels, see the Configuring Passwords and Privileges chapter in the Cisco IOS Security Configuration Guide.)

How to Configure and Use the Cisco IOS Web Browser User Interface

Enabling the Cisco IOS Web Browser UI

To enable the Cisco Web browser UI, you must enable the HTTP server on your router:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
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 server (web server) on the system.

Configuring Access to the Cisco IOS Web Browser UI

To control access to the Cisco Web browser UI, you can specify the authentication method for the HTTP server, apply an access list to the HTTP server, and assign a port number for the HTTP server, as described in the following sections.

Specifying the Method for User Authentication

To specify how HTTP server users are authenticated, use the following command in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http authentication** {**aaa**|**enable** | **local** | **tacacs**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http authentication** {**aaa**|**enable**	**local**	**tacacs**} **Example:** `Router(config)# ip http authentication tacacs`	Specifies how the HTTP server users are authenticated.

Example

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
```

Applying an Access List to the HTTP Server

To control which hosts can access the HTTP server used by the Cisco Web browser UI, you can apply an access list:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http access-class** {*access-list-number* |*access-list-name* }

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http access-class** {*access-list-number* |*access-list-name* } **Example:** `Router(config)# ip http access-class 20`	Applies an access list to the HTTP server used by the Cisco IOS ClickStart software or the Cisco Web browser user interface.

Example

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
```

Changing the HTTP Server Port Number

By default, the HTTP server uses port 80 on the router. To assign the Cisco Web browser UI to a different port, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http port** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http port** *number* **Example:** `Router(config)# ip http port 32`	Assigns a port number to be used by the Cisco IOS Web browser interface.

Accessing and Using the Cisco IOS Web Browser UI

This section describes the tasks used to access the Cisco IOS Web browser UI and issue commands:

Accessing the Router Home Page

To access a router home page, perform the following steps:

SUMMARY STEPS

1. Enter **http://***router-name***/** in the URL field of your Web browser and press **Return** . (For example, to access a Cisco router named cacophony, type **http://cacophony/**.) The browser then prompts you for the password.
2. Enter the password. The required password is dependent on the user authentication method configured for the HTTP server (using the **ip http authentication** global configuration command).

DETAILED STEPS

Step 1 Enter **http://***router-name***/** in the URL field of your Web browser and press **Return** . (For example, to access a Cisco router named cacophony, type **http://cacophony/**.) The browser then prompts you for the password.

Step 2 Enter the password. The required password is dependent on the user authentication method configured for the HTTP server (using the **ip http authentication** global configuration command).

After entering the password, the browser displays the router home page.

Changing the Default Privilege Level

To access a router Web page for a preassigned privilege level other than the default of 15, perform the following steps:

SUMMARY STEPS

1. E nter **http://***router-name***/level/***level***/exec** in the URL field of your Web browser and press **Return**. For example, to request access to EXEC mode at user privilege level of 12 on a Cisco router named cacophony, type **http://cacophony/level/12/exec**. The browser will then prompt you for your username and password.
2. Enter your username and password and press **Return**. The required password is dependent on the user authentication method configured for the HTTP server. The Web browser will display a Web page specific to your user privilege level.

DETAILED STEPS

Step 1 E nter **http://***router-name***/level/***level***/exec** in the URL field of your Web browser and press **Return**. For example, to request access to EXEC mode at user privilege level of 12 on a Cisco router named cacophony, type **http://cacophony/level/12/exec**. The browser will then prompt you for your username and password.

Step 2 Enter your username and password and press **Return**. The required password is dependent on the user authentication method configured for the HTTP server. The Web browser will display a Web page specific to your user privilege level.

Configuration Examples for the Cisco IOS Web Browser User Interface

Example SSI EXEC Command

The following example shows how the HTML SSI EXEC command can be used to execute a command. In this example, the Cisco IOS **showusers** EXEC command is executed.

The contents of the HTML file in Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
<PRE>
<!--#exec cmd="show users"-->
</PRE>
<BR>
</BODY>
</HTML>
```

The contents that the Web browser receives when the HTML file is retrieved from Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
USERS:<BR>
<PRE>
Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com
</PRE>
<BR>
</BODY>
</HTML>
```

The Web browser shows the following text:

```
This is an example of the SSI EXEC command
-----------------------------------------
USERS:
Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com
```

Example SSI ECHO Command

The following is an example of the HTML SSI ECHO command used with the SSI variable *SERVER_NAME* to display the Cisco IOS platform host name “rain.”

The contents of the HTML file in Flash memory is as follows:

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
<!--#echo var="SERVER_NAME"-->
<BR>
</BODY>
</HTML>
```

The contents that the Web browser receives when the HTML file is retrieved from Flash memory are as follows:

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
rain
<BR>
</BODY>
</HTML>
```

The Web Browser shows the following text:

```
This is an example of the SSI echo command
-----------------------------------------
The name of this server is:
rain
```