



## clear ip http client cookie through show ip http server secure status

---

- [ip http access-class, page 3](#)
- [ip http accounting commands, page 5](#)
- [ip http authentication, page 7](#)
- [ip http client connection, page 10](#)
- [ip http client password, page 12](#)
- [ip http client proxy-server, page 14](#)
- [ip http client response, page 16](#)
- [ip http client secure-ciphersuite, page 18](#)
- [ip http client secure-trustpoint, page 20](#)
- [ip http client source-interface, page 22](#)
- [ip http client username, page 24](#)
- [ip http max-connections, page 26](#)
- [ip http path, page 28](#)
- [ip http port, page 30](#)
- [ip http secure-ciphersuite, page 32](#)
- [ip http secure-client-auth, page 34](#)
- [ip http secure-port, page 36](#)
- [ip http secure-server, page 38](#)
- [ip http secure-trustpoint, page 40](#)
- [ip http server, page 42](#)
- [ip http timeout-policy, page 44](#)
- [show ip http client, page 47](#)
- [show ip http client connection, page 51](#)

- [show ip http client history, page 53](#)
- [show ip http client secure status, page 55](#)
- [show ip http client session-module, page 57](#)
- [show ip http server, page 60](#)
- [show ip http server secure status, page 64](#)

# 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 <b>access-list</b> global configuration command. |
|---------------------------|--|

## Command Default

No access list is applied to the HTTP server.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification  |
|-------------|---|
| 11.2        | This command was introduced.  |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.   |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## 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 shows how to define an access list as 20 and assign it to the HTTP server:

```
Router(config)# ip access-list standard 20
```

```

Router(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Router(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Router(config-std-nacl)# permit 209.165.200.225 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  |
|-----------------------|--|
| <b>ip access-list</b> | Assigns an ID to an access list and enters access list configuration mode.   |
| <b>ip http server</b> | Enables the HTTP 1.1 server, including the Cisco web browser user interface. |

## ip http accounting commands

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

**ip http accounting commands** *level* {**default**|*named-accounting-method-list*}

**no ip http accounting commands** *level*

### Syntax Description

|                                     |  |
|-------------------------------------|--|
| <i>level</i>                        | Indicates a privilege value from 0 to 15. By default, the following command privilege levels are available on the router: <ul style="list-style-type: none"> <li>• 0—Includes the <b>disable</b>, <b>enable</b>, <b>exit</b>, <b>help</b>, and <b>logout</b> commands.</li> <li>• 1—Includes all user-level commands at the router prompt (&gt;).</li> <li>• 15—Includes all enable-level commands at the router prompt (&gt;).</li> </ul> |
| <b>default</b>                      | Indicates the <b>default</b> accounting method list configured by the <b>aaa accounting</b> commands.  |
| <i>named-accounting-method-list</i> | Name of the predefined command accounting method list.   |

### Command Default

Command accounting for HTTP and HTTP over Secure Socket Layer (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 **ip http accounting commands** can be used to configure HTTP and HTTPS to use any predefined AAA method list.

### Command Modes

Global configuration (config)

### Command History

| Release     | Modification  |
|-------------|---|
| 12.4(15)T   | This command was introduced.                                    |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

| Release    | Modification   |
|------------|--|
| 12.2(50)SY | This command was integrated into Cisco IOS Release 12.2(50)SY. |

### Usage Guidelines

Command accounting provides information about the commands, executed on a device, for a specified privilege level. Each command accounting record corresponds to one IOS command executed at its respective privilege level, the date and time the command was executed, and the user who executed it. Command accounting will be implemented for HTTP and HTTPS. A stop accounting record will be generated for any command execution/configuration done by a user via HTTP and HTTPS.

If this command is not configured, HTTP and HTTPS will use the default AAA accounting list whenever AAA is enabled using the **aaa new-model** configuration command. If the default method list does not exist, no accounting records will be generated. Whenever AAA is disabled, no accounting records will be generated.



#### Note

The above behavior is essential to maintain the consistency of HTTP and HTTPS accounting CLI with their counterparts available for Telnet/SSH in IOS line configuration mode.

### Examples

The following example shows how to configure HTTP and HTTPS to allow AAA accounting support:

```
Router(config)# ip http accounting commands 1 oneacct
```

### Related Commands

| Command                           | Description  |
|-----------------------------------|--|
| <b>aaa authentication login</b>   | Specifies the login authentication method to be used by the AAA service. |
| <b>aaa authorization</b>          | Sets parameters that restrict user access to a network.                  |
| <b>aaa new-model</b>              | Enables the AAA access control model.                                    |
| <b>ip http authentication aaa</b> | Specifies a particular authentication method for HTTP server users.      |
| <b>ip http server</b>             | Enables the HTTP server.   |

# 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 {**command-authorization** *level listname*| **exec-authorization** *listname*| **login-authentication** *listname*}}| **enable**| **local**| **tacacs**}

**no ip http authentication** {aaa {**command-authorization** *level listname*| **exec-authorization** *listname*| **login-authentication** *listname*}}| **enable**| **local**| **tacacs**}

## Syntax Description

|                               |  |
|-------------------------------|--|
| <b>aaa</b>                    | Indicates that the authentication method used for the authentication, authorization, and accounting (AAA) login service should be used for authentication. The AAA login authentication method is specified by the <b>aaa authentication login default</b> command, unless otherwise specified by the <b>login-authentication listname</b> keyword and argument.   |
| <b>command- authorization</b> | Sets the authorization method list for commands at the specified privilege level.  |
| <i>level</i>                  | Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router: <ul style="list-style-type: none"> <li>• 0--Includes the <b>disable</b>, <b>enable</b>, <b>exit</b>, <b>help</b>, and <b>logout</b> commands.</li> <li>• 1--Includes all user-level commands at the router prompt (&gt;).</li> <li>• 15--Includes all enable-level commands at the router prompt (&gt;).</li> </ul> |
| <i>listname</i>               | Sets the name of the method list.  |
| <b>exec- authorization</b>    | Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session.   |
| <b>login- authentication</b>  | Sets the method list for login authentication, which enables AAA authentication for logins.  |
| <b>enable</b>                 | Indicates that the “enable” password should be used for authentication. (This is the default method.)  |

|               |  |
|---------------|--|
| <b>local</b>  | Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the <b>username</b> global configuration command) should be used for authentication and authorization. |
| <b>tacacs</b> | Indicates that the TACACS (or XTACACS) server should be used for authentication.   |

**Command Default**

The “enable” password is required when users (clients) connect to the HTTP server. Three command privilege levels exist on the router.

**Command Modes**

Global configuration (config)

**Command History**

| Release     | Modification   |
|-------------|--|
| 11.2 F      | This command was introduced.   |
| 12.3(8)T    | The <b>tacacs</b> keyword was removed. The <b>command-authorization</b> , <b>exec-authorization</b> , and <b>login-authentication</b> keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.  |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.  |

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



## Examples

The following example shows how to specify that AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method. This example also shows how to specify using the local username database for login authentication and EXEC authorization of HTTP sessions:

```
Router(config)# aaa authentication login LOCALDB local
Router(config)# aaa authorization exec LOCALDB local
Router(config)# ip http authentication aaa login-authentication LOCALDB
Router(config)# ip http authentication aaa exec-authorization LOCALDB
```

## Related Commands

| Command                         | Description  |
|---------------------------------|--|
| <b>aaa authentication login</b> | Specifies the login authentication method to be used by the AAA service. |
| <b>aaa authorization</b>        | Sets parameters that restrict user access to a network.                  |
| <b>ip http server</b>           | Enables the HTTP server.   |

## ip http client connection

To configure an HTTP client connection to a remote HTTP server for file transfers, use the **ip http client connection** command in global configuration mode. To remove the configuration, use the **no** form of this command.

**ip http client connection** {forceclose| idle timeout *seconds*| pipeline-length *length*| retry *count*| timeout *seconds*}

**no ip http client connection** {forceclose| idle| pipeline-length| retry| timeout}

### Syntax Description

|                        |   |
|------------------------|---|
| <b>forceclose</b>      | Disables a persistent connection.<br><br>HTTP persistent connection, also called HTTP keepalive or HTTP connection reuse, uses the same TCP connection to send and receive multiple HTTP requests instead of opening a new connection for every single request. |
| <b>idle timeout</b>    | Sets the idle time before the connection between an HTTP client and a server is closed.   |
| <i>seconds</i>         | Time, in seconds. Range: 1 to 60. Default: 30.  |
| <b>pipeline-length</b> | Defines the maximum number of HTTP requests that can be queued to a server without getting a response.  |
| <i>length</i>          | Maximum number of HTTP requests. Range: 2 to 100.   |
| <b>retry</b>           | Sets the retry count in the case of a connection establishment timeout. Range: 1 to 5. Default: 1.  |
| <i>count</i>           | Number of connection attempts. Range: 1 to 5. Default: 1.   |
| <b>timeout</b>         | Sets the maximum time that an HTTP client waits for a connection.   |
| <i>seconds</i>         | Maximum time, in seconds, that an HTTP client waits for a connection. Range: 1 to 60. Default: 10.  |

**Command Default** A persistent connection is enabled.

**Command Modes** Global configuration (config)

**Command History**

| Release     | Modification   |
|-------------|--|
| 12.3(7)T    | This command was introduced.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.  |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.  |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.   |
| 15.0(1)M    | This command was modified. The <b>pipeline-length</b> keyword and the <i>length</i> argument were added. |

**Examples**

The following example shows how to configure an idle connection time of 15 seconds for an HTTP client persistent connection.

```
Router(config)# ip http client connection idle timeout 15
```

**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for an HTTP client.   |
| <b>ip http client cache</b>            | Configures an HTTP client cache.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client response</b>         | Configures the time for which an HTTP client waits for a response from the server for a request message.   |
| <b>ip http client source-interface</b> | Configures a source interface for an HTTP client.  |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |
| <b>show ip http client</b>             | Displays HTTP client information.  |

# ip http client password

To configure the default password used for connections to remote HTTP servers, use the **ip http client password** command in global configuration mode. To remove a configured default password from the configuration, use the **no** form of this command.

```
ip http client password {0 password| 7 password| password}
no ip http client password
```

## Syntax Description

|          |  |
|----------|--|
| 0        | 0 specifies that an unencrypted password follows. The default is an unencrypted password.      |
| 7        | 7 specifies that an encrypted password follows.  |
| password | The password string to be used in HTTP client connection requests sent to remote HTTP servers. |

## Command Default

No default password exists for the HTTP connections.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification   |
|-------------|--|
| 12.3(2)T    | This command was introduced.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.  |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.  |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.   |
| 15.0(1)M    | This command was modified in a release earlier than Cisco IOS 15.0(1)M. The 0 and 7 keywords were added. |

## Usage Guidelines

This command is used to configure a default password before a file is downloaded from a remote web server using the **copy http://** or **copy https://** command. The default password will be overridden by a password specified in the URL of the **copy** command.

The password is encrypted in the configuration files.

**Note**

The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

**Examples**

In the following example, the default HTTP password is configured as Password and the default HTTP username is configured as User2 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Password
Router(config)# ip http client username User2
Router(config)# do show running-config | include ip http client
```

**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client cache</b>            | Configures the HTTP client cache.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client response</b>         | Configures HTTP client characteristics for managing HTTP server responses to request messages.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |
| <b>show ip http client</b>             | Displays a report about the HTTP client.   |

# ip http client proxy-server

To configure an HTTP proxy server, use the **ip http client proxy-server** command in global configuration mode. To disable or change the proxy server, use the **no** form of this command.

**ip http client proxy-server** *proxy-name* **proxy-port** *port-number*

**no ip http client proxy-server**

## Syntax Description

|                    |   |
|--------------------|---|
| <i>proxy-name</i>  | Name of the proxy server.   |
| <b>proxy-port</b>  | Specifies a proxy port for HTTP file system client connections.                             |
| <i>port-number</i> | Integer in the range of 1 to 65535 that specifies a port number on the remote proxy server. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification  |
|-------------|---|
| 12.3(7)T    | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## Usage Guidelines

This command configures the HTTP client to connect to a remote proxy server for HTTP file system client connections.

## Examples

The following example shows how to configure the HTTP proxy server named edge2 at port 29:

```
Router(config)# ip http client proxy-server edge2 proxy-port 29
```

**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client cache</b>            | Configures the HTTP client cache.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client response</b>         | Configures HTTP client characteristics for managing HTTP server responses to request messages.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |
| <b>show ip http client</b>             | Displays a report about the HTTP client.   |

## ip http client response

To configure the number of seconds that the HTTP client waits for a response from the server for a request message, use the **ip http client response** command in global configuration mode. To remove the specified number of seconds that the HTTP client waits for a response, use the **no** form of this command.

**ip http client response timeout** *seconds*

**no ip http client response timeout**

### Syntax Description

|                |   |
|----------------|---|
| <b>timeout</b> | Specifies a response timeout period.  |
| <i>seconds</i> | The amount of time, in seconds, to wait for a response to a domain name system (DNS) query. The range is from 1 to 300. |

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

| Release     | Modification  |
|-------------|---|
| 12.2(15)T   | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

### Usage Guidelines

Use this command to specify the response timeout value.

### Examples

The following example shows how to specify a response timeout of 180 seconds:

```
Router(config)# ip http client response timeout 180
```



**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client cache</b>            | Configures the HTTP client cache.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |
| <b>show ip http client</b>             | Displays a report about the HTTP client.   |

## 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

|                         |   |
|-------------------------|---|
| <b>3des-ede-cbc-sha</b> | SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest. |
| <b>rc4-128-sha</b>      | 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.                             |
| <b>rc4-128-md5</b>      | SSL_RSA_WITH_RC4_128_MD5--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.          |
| <b>des-cbc-sha</b>      | SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.  |

### Command Default

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.                                    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

### 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 CipherSuites 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

The following example shows how to configure the HTTPS client 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  |
|--|--|
| <b>show ip http client secure status</b> | Displays the configuration status of the secure HTTP client. |

## ip http client secure-trustpoint

To specify the remote certificate authority (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 <b>crypto ca trustpoint</b> command. |
|------------------------|--|

### Command Default

If the remote HTTPS server requests client certification, the secure HTTP client will use the trustpoint configured using the **primary** command 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.                                    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

### 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 HTTPS client for cases when the remote HTTPS server requires client authorization.

Use this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode 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 attempts to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** command.

## Examples

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

```
!The following commands specify 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   |
|-----------------------------|---|
| <b>crypto ca trustpoint</b> | Specifies a name for a certificate authority trustpoint and enters CA trustpoint configuration mode.  |
| <b>primary</b>              | Indicates that the CA trustpoint being configured should be used as the primary (default) trustpoint. |

# ip http client source-interface

To configure a source interface for the HTTP client, use the **ip http client source-interface** command in global configuration mode. To change or disable the source interface, use the **no** form of this command.

**ip http client source-interface** *type number*

**no ip http client source-interface**

## Syntax Description

|               |                                 |
|---------------|---------------------------------|
| <i>type</i>   | Name of the source interface.   |
| <i>number</i> | Number of the source interface. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification  |
|-------------|---|
| 12.3(7)T    | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## Usage Guidelines

Use this command to specify a source interface to use for HTTP connections.

## Examples

The following example shows how to configure the source interface as Ethernet 0/1:

```
Router(config)# ip http client source-interface Ethernet 0/1
```

## Related Commands

| Command     | Description  |
|-------------|--|
| <b>copy</b> | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |

| Command                            | Description  |
|------------------------------------|--|
| <b>debug ip http client</b>        | Enables debugging output for the HTTP client.  |
| <b>ip http client cache</b>        | Configures the HTTP client cache.  |
| <b>ip http client connection</b>   | Configures the HTTP client connection.   |
| <b>ip http client password</b>     | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b> | Configures an HTTP proxy server.   |
| <b>ip http client response</b>     | Configures HTTP client characteristics for managing HTTP server responses to request messages. |
| <b>ip http client username</b>     | Configures a login name for all HTTP client connections.                                       |
| <b>show ip http client</b>         | Displays a report about the HTTP client.   |

# ip http client username

To configure the default username used for connections to remote HTTP servers, use the **ip http client username** command in global configuration mode. To remove a configured default HTTP username from the configuration, use the **no** form of this command.

**ip http client username** *username*

**no ip http client username**

## Syntax Description

|                 |   |
|-----------------|---|
| <i>username</i> | String that is the username (login name) to be used in HTTP client connection requests sent to remote HTTP servers. |
|-----------------|---|

## Command Default

No default username exists for the HTTP connections.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification  |
|-------------|---|
| 12.3(2)T    | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## Usage Guidelines

This command is used to configure a default username before a file is copied to or from a remote web server using the **copy http://** or **copy https://** command. The default username will be overridden by a username specified in the URL of the **copy** command.



### Note

The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

## Examples

In the following example, the default HTTP password is configured as Secret and the default HTTP username is configured as User1 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Secret
Router(config)# ip http client username User1
```



**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client cache</b>            | Configures the HTTP client cache.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client response</b>         | Configures HTTP client characteristics for managing HTTP server responses to request messages.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>show ip http client</b>             | Displays a report about the HTTP client.   |

# 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**

## Syntax Description

|              |  |
|--------------|--|
| <i>value</i> | An integer in the range from 1 to 16 that specifies the maximum number of concurrent HTTP connections. The default is 5. |
|--------------|--|

## Command Default

Five concurrent HTTP connections is the default.

## Command Modes

Global configuration (config)

## Command History

| Release     | Modification  |
|-------------|---|
| 12.2(15)T   | This command was introduced.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## Usage Guidelines

Platform-specific implementations can supersede 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 new connections until the current number of connections falls below the new configured value.

## Examples

The following example shows how to configure the HTTP server to allow up to 10 simultaneous connections:

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

**Related Commands**

| Command               | Description  |
|-----------------------|--|
| <b>ip http server</b> | 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 remove the base path specification, use the **no** form of this command.

**ip http path** *url*

**no ip http path**

### Syntax Description

|            |  |
|------------|--|
| <i>url</i> | Cisco IOS File System (IFS) URL specifying the location of the HTML files used by the HTTP server. |
|------------|--|

### Command Default

The HTTP server is disabled.

### Command Modes

Global configuration (config)

### Command History

| Release     | Modification  |
|-------------|---|
| 12.0        | This command was introduced.  |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.   |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

### Usage Guidelines

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 path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

### Examples

In the following example, the HTML files are located in the default flash location on the system:

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

In the following example, the HTML files are located in the directory named web on the flash memory card inserted in slot 0:

```
Router(config)# ip http path slot0:web
```

#### Related Commands

| Command               | Description  |
|-----------------------|--|
| <b>ip http server</b> | 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**

## Syntax Description

|                    |   |
|--------------------|---|
| <i>port-number</i> | The integer 80 or any integer in the range from 1025 to 65535 that specifies the port number to be used for the HTTP server. The default is 80. |
|--------------------|---|

## Command Default

The HTTP server uses port 80.

## Command Modes

Global configuration (config)

## 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 secure HTTP (HTTPS) connections.  |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2.   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.   |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## Usage Guidelines

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



### Note

The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

## Examples

The following example shows how to change the HTTP server port to port 8080:

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

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

## Related Commands

| Command               | Description  |
|-----------------------|--|
| <b>ip http server</b> | 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--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (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 Message Digest 5 (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.  |

## Command Default

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

## Command Modes

Global configuration

## Command History

| Release     | Modification  |
|-------------|---|
| 12.2(15)T   | This command was introduced.                                    |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |



## 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 CipherSuites 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 12.2(15)T.

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 Sockets Layer (SSL) 3.0 protocol.

## Examples

The following example shows how to restrict 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  |
|--|--|
| <b>ip http secure-server</b>             | Enables the HTTPS server.                                    |
| <b>show ip http server secure status</b> | Displays the configuration status of the secure HTTP server. |

# ip http secure-client-auth

To configure the secure HTTP server 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.

**Command Default** 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.                                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**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  |
|--|--|
| <b>ip http secure-server</b>             | Enables the HTTPS server.                                    |
| <b>show ip http server secure status</b> | Displays the configuration status of the secure HTTP server. |

# ip http secure-port

To set the secure HTTP (HTTPS) server port number for listening, use the **ip http secure-port** command in global configuration mode. To return the HTTPS 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 | <div><div>port-number</div><div>Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.</div></div> |
|--------------------|--|

Command Default

The HTTPS server port number is not set for listening.

Command Modes

Global configuration

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.1(11b)E  | This command was introduced.                                    |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.   |
|                 | 12.2(15)T   | This command was integrated into Cisco IOS Release 12.2(15)T.   |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

Usage Guidelines

An HTTP server and an HTTPS server cannot use the same port. If you try to configure both on the same port, the following message is displayed:

```
% Port port_number in use by HTTP.
where port_number is the port number that is already assigned to the HTTP server.
```

If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

```
https://device:port_number
```

where port\_number is the HTTPS port number.

## Examples

The following example shows how to assign port 1025 for HTTPS server connections:

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

## Related Commands

| Command               | Description              |
|-----------------------|--------------------------|
| ip http secure-server | Enables an HTTPS server. |

# ip http secure-server

To enable a secure HTTP (HTTPS) server, use the **ip http secure-server** command in global configuration mode. To disable an HTTPS 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.

**Command Default** The HTTPS server is disabled.

**Command Modes** Global configuration

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.1(11b)E  | This command was introduced.                                    |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.   |
|                 | 12.2(15)T   | This command was integrated into Cisco IOS Release 12.2(15)T.   |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**Usage Guidelines** The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.



## Note

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

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

**Examples** In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Router# configure 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
```

## Related Commands

| Command                                  | Description   |
|--|---|
| <b>ip http secure-trustpoint</b>         | Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server. |
| <b>ip http server</b>                    | Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.        |
| <b>show ip http server secure status</b> | Displays the configuration status of the HTTPS server.  |

# ip http secure-trustpoint

To specify the certificate authority (CA) trustpoint that should be used for obtaining signed certificates for a secure HTTP (HTTPS) 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 | <table><tr><td>trustpoint-name</td><td>Name of a configured trustpoint. Use the same trustpoint name that was used in the associated <b>crypto ca trustpoint</b> command.</td></tr></table> | trustpoint-name | Name of a configured trustpoint. Use the same trustpoint name that was used in the associated <b>crypto ca trustpoint</b> command. |
| trustpoint-name    | Name of a configured trustpoint. Use the same trustpoint name that was used in the associated <b>crypto ca trustpoint</b> command.  |                 |  |

|                 |  |
|-----------------|--|
| Command Default | The HTTPS server uses the trustpoint configured when you use the <b>primary</b> command. If a trustpoint is not configured, the HTTPS server uses a self-signed certificate. |
|-----------------|--|

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

| Command History | <table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(15)T</td><td>This command was introduced.</td></tr><tr><td>12.2(33)SRA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td></tr><tr><td>12.2(33)SXH</td><td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td></tr><tr><td>12.2(33)SB</td><td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td></tr></table> | Release | Modification | 12.2(15)T | This command was introduced. | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. | 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |
|-----------------|--|---------|--------------|-----------|------------------------------|-------------|---|-------------|---|------------|--|
| Release         | Modification   |         |              |           |                              |             |   |             |   |            |  |
| 12.2(15)T       | This command was introduced.   |         |              |           |                              |             |   |             |   |            |  |
| 12.2(33)SRA     | This command was integrated into Cisco IOS Release 12.2(33)SRA.  |         |              |           |                              |             |   |             |   |            |  |
| 12.2(33)SXH     | This command was integrated into Cisco IOS Release 12.2(33)SXH.  |         |              |           |                              |             |   |             |   |            |  |
| 12.2(33)SB      | This command was integrated into Cisco IOS Release 12.2(33)SB.   |         |              |           |                              |             |   |             |   |            |  |

**Usage Guidelines**

This command specifies that the HTTPS 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 this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode commands. If a trustpoint is not configured, the HTTPS 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** command.



## Examples

In the following example, the CA trustpoint is configured, a certificate is obtained, and the certificate is referenced in the HTTPS 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

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   |
|--|---|
| <b>crypto ca trustpoint</b>              | Declares the CA that your routing device should use.                    |
| <b>ip http secure-server</b>             | Enables the HTTPS server.   |
| <b>primary</b>                           | Assigns a specified trustpoint as the primary trustpoint of the router. |
| <b>show ip http server secure status</b> | Displays the configuration status of the secure HTTP server.            |

# ip http server

To enable the HTTP server on your IP or IPv6 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.

## Command Default

The HTTP server is disabled on the Cisco Catalyst 4000 series switch. The HTTP server is enabled for clustering on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

The HTTP server uses the standard port 80 by default.

## Command Modes

Global configuration (config)

## Command History

| Release                  | Modification  |
|--------------------------|---|
| 11.2                     | This command was introduced.  |
| 12.2(2)T                 | IPv6 support was added.   |
| 12.2(15)T                | The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.  |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.   |
| 12.2(31)SB2              | This command was integrated into Cisco IOS Release 12.2(31)SB2.   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC              | This command was integrated into Cisco IOS Release 12.2(33)SRC.   |
| 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers.   |
| 12.4(24)T                | Support for IPv6 Secure Neighbor Discovery (SeND) was added.  |

### Usage Guidelines

With IPv6 support added in Cisco IOS Release 12.2(2)T, the **ip http server** command simultaneously enables and disables both IP and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command will only be applied to IPv4 traffic. IPv6 traffic filtering is not supported.



### Caution

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

### Examples

The following example shows how to enable the HTTP server on both IP and IPv6 systems:

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

### Related Commands

| Command                      | Description  |
|------------------------------|--|
| <b>ip http access-class</b>  | Specifies the access list that should be used to restrict access to the HTTP server. |
| <b>ip http path</b>          | Specifies the base path used to locate files for use by the HTTP server.             |
| <b>ip http secure-server</b> | Enables the HTTPS 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     | Specifies the maximum number of seconds that a connection will be kept open if no data is received or response data cannot be sent out.  |
| life     | Specifies the maximum number of seconds that a connection will be kept open from the time the connection is established.   |
| seconds  | When used with the <b>idle</b> keyword, an integer in the range of 1 to 600 that specifies the number of seconds (10 minutes maximum). The default is 180 (3 minutes).<br><br>When used with the <b>life</b> keyword, an integer in the range of 1 to 86400 that specifies the number of seconds (24 hours maximum). The default is 180 (3 minutes). |
| requests | Specifies that a maximum limit is set on the number of requests processed on a persistent connection before it is closed.  |
| value    | Integer in the range from 1 to 86400. The default is 1.  |

## Command Default

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 (config)

## Command History

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

| Release     | Modification  |
|-------------|---|
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## 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.

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 **requests** 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 **requests** 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 for 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 for 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  |
|-----------------------|--|
| <b>ip http server</b> | Enables the HTTP server, including the Cisco web browser user interface. |

# show ip http client

To display a report about the HTTP client, use the **show ip http client** command in user EXEC or privileged EXEC mode.

**show ip http client** {**all**|**cache**|**connection**|**history**|**secure status**|**session-module**|**statistics**}

## Syntax Description

|                       |  |
|-----------------------|--|
| <b>all</b>            | Displays a report that contains all of the information available about the HTTP client: status (enabled or disabled), registered application or session modules, active connections, cache, history, and statistics. |
| <b>cache</b>          | Displays a list of information about the HTTP client cache.  |
| <b>connection</b>     | Displays HTTP client active connections and configured values for connections.   |
| <b>history</b>        | Displays a list of up to 20 URLs most recently accessed by the HTTP client.  |
| <b>secure status</b>  | Displays the status of the secure HTTP client configuration.<br><br><b>Note</b> This keyword is not supported with Cisco IOS Release 12.2(31)SB2.  |
| <b>session-module</b> | Displays a report about sessions or applications that have registered with the HTTP client.  |
| <b>statistics</b>     | No statistics are collected for the HTTP client. This feature will be implemented at a later date.   |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release     | Modification   |
|-------------|--|
| 12.3(2)T    | This command was introduced.   |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. The <b>all</b> , <b>cache</b> , and <b>statistics</b> keywords were added. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC.  |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.   |

**Usage Guidelines**

Use this command to display information about the HTTP client.

**Note**

The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

**Examples**

The following is sample output from the **show ip http client cache** command:

```
Router# show ip http client cache
```

```
HTTP client cache:
Maximum Memory size for cache      : 100000 bytes (default)
Maximum memory per cache entry     : 2000 bytes (default)
Memory used                        : 1381 bytes
Memory Available                   : 98619 bytes
Cache Ager interval                : 5 minutes (default)
Total entries created              : 2
```

| Id  | Type | Url                | Memory-size (Bytes) | Refcnt | Valid (Sec) |
|-----|------|--------------------|---------------------|--------|-------------|
| 536 | Hdr  | 172.25.125.69/     | 673                 | 0      | -1          |
| 32  | Hdr  | 172.25.125.7:8888/ | 708                 | 0      | -1          |

The report is self-explanatory and lists information about the cache.

The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection
HTTP client current connections:
  Persistent connection = enabled (default)
  Connection establishment timeout = 10s (default)
  Connection idle timeout = 30s (default)
  Maximum number of connection establishment retries = 1 (default)
  Maximum http client connections per host : 2
  HTTP secure client capability: Not present

  local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
                        :80      172.20.67.174:11012 12584     176

  Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history
HTTP client history:
  GET 03:25:36 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
  GET 03:25:56 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
  GET 03:26:10 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status
HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

The table below describes the significant fields shown in the display.



**Table 1: show ip http client secure status Field Descriptions**

| Field                           | Description   |
|---------------------------------|---|
| HTTP secure client ciphersuite: | Displays the configuration of the <b>ip http client secure-ciphersuite</b> command. |
| HTTP secure client trustpoint:  | Displays the configuration of the <b>ip http client secure-trustpoint</b> command.  |

The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module
HTTP client application session modules:
Id                :1
Application Name   :HTTP CFS
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout  :0
Retries           :0
Proxy             :
Id                :6
Application Name   :httpc_ifs_0
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout  :16
Retries           :0
Proxy             :
```

The table below describes the fields shown in the display.

## Related Commands

**Table 2: show ip http client session-module Field Descriptions**

| Field            | Description  |
|------------------|--|
| Id               | A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.   |
| Application Name | Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session (CFS) application, and the name httpc_ifs_0 is the HTTP client (HTTPC) Cisco IOS File System (IFS) Copy application. |
| Version          | HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP 1.0 does not support persistent connections; HTTP 1.1 supports both persistent and nonpersistent connections.   |

| Field            | Description  |
|------------------|--|
| Persistent       | Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer. |
| Response-timeout | Configured response timeout period, in seconds. The application specifies the amount of time the HTTP client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.  |
| Retries          | Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.   |
| Proxy            | Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.  |

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |

# show ip http client connection

To display a report about HTTP client active connections, use the **show ip http client connection** command in privileged EXEC mode.

**show ip http client connection**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.3(2)T    | This command was introduced.                                    |
|                 | 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | 12.4(20)T   | This command was integrated into Cisco IOS Release 12.4(20)T.   |

**Usage Guidelines** Use this command to display active connections and configured values for connections.

**Examples** The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection
HTTP client current connections:
  Persistent connection = enabled (default)
  Connection establishment timeout = 10s (default)
  Connection idle timeout = 30s (default)
  Maximum number of connection establishment retries = 1 (default)
  Maximum http client connections per host : 2
  HTTP secure client capability: Not present

  local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
                        :80      172.20.67.174:11012 12584      176

  Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

**Related Commands**

| Command                                   | Description  |
|---|--|
| <b>copy</b>                               | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>               | Enables debugging output for the HTTP client.  |
| <b>ip http client connection</b>          | Configures the HTTP client connection.   |
| <b>ip http client password</b>            | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>        | Configures an HTTP proxy server.   |
| <b>ip http client source-interface</b>    | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>            | Configures a login name for all HTTP client connections.   |
| <b>show ip http client history</b>        | Displays the URLs accessed by the HTTP client.   |
| <b>show ip http client session-module</b> | Displays a report about sessions that have registered with the HTTP client.  |

# show ip http client history

To display up to 20 URLs accessed by the HTTP client, use the **show ip http client history** command in privileged EXEC mode.

**show ip http client history**

**Syntax Description** This command has no arguments or keywords

**Command Default** No default behavior or values

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.3(2)T    | This command was introduced.                                    |
|                 | 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**Usage Guidelines** This command displays a list of up to 20 URLs most recently accessed by the HTTP client.

**Examples** The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history
HTTP client history:
  GET 03:25:36 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
  GET 03:25:56 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
  GET 03:26:10 UTC Thu Feb 26 2004
  mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

**Related Commands**

| Command                     | Description  |
|-----------------------------|--|
| <b>copy</b>                 | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b> | Enables debugging output for the HTTP client.  |

| Command                                   | Description   |
|---|---|
| <b>ip http client connection</b>          | Configures the HTTP client connection.                                      |
| <b>ip http client password</b>            | Configures a password for all HTTP client connections.                      |
| <b>ip http client proxy-server</b>        | Configures an HTTP proxy server.  |
| <b>ip http client source-interface</b>    | Configures a source interface for the HTTP client.                          |
| <b>ip http client username</b>            | Configures a login name for all HTTP client connections.                    |
| <b>show ip http client connection</b>     | Displays a report about HTTP client active connections.                     |
| <b>show ip http client session-module</b> | Displays a report about sessions that have registered with the HTTP client. |

## show ip http client secure status

To display the status of the secure HTTP client configuration, use the **show ip http client secure status** command in privileged EXEC mode.

**show ip http client secure status**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.2(15)T   | This command was introduced.                                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**Examples** The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status
HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

The table below describes the significant fields shown in the display.

**Table 3: show ip http client secure status Field Descriptions**

| Field                           | Description   |
|---------------------------------|---|
| HTTP secure client ciphersuite: | Displays the configuration of the <b>ip http client secure-ciphersuite</b> command. |
| HTTP secure client trustpoint:  | Displays the configuration of the <b>ip http client secure-trustpoint</b> command.  |

**Related Commands**

| Command                                 | Description   |
|---|---|
| ip http client secure-ciphersuite       | Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the client to a remote server. |
| <b>ip http client secure-trustpoint</b> | Specifies the CA trustpoint that should be used if the remote HTTP server requests client authentication.                         |



# show ip http client session-module

To display a report about sessions or applications that have registered with the HTTP client, use the **show ip http client session-module** command in privileged EXEC mode.

**show ip http client session-module**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.3(2)T    | This command was introduced.                                    |
|                 | 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**Usage Guidelines** Use this command to display information about applications that have registered with the HTTP client.

**Examples** The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module
HTTP client application session modules:
Id                :1
Application Name   :HTTP CFS
Version           :HTTP/1.0
Persistent        :non-persistent
Response-timeout  :0
Retries           :0
Proxy             :
Id                :6
Application Name   :httpc_ifs_0
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout  :16
Retries           :0
Proxy             :
```

The table below describes the fields shown in the display.

**Table 4: show ip http client session-module Field Descriptions**

| Field            | Description  |
|------------------|--|
| Id               | A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.   |
| Application Name | Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session application, and the name httpc_ifs_0 is the HTTPC IFS Copy application.       |
| Version          | HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP1.0 does not support persistent connections; HTTP1.1 supports both persistent and nonpersistent connections.         |
| Persistent       | Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer. |
| Response-timeout | Configured response timeout period, in seconds. The application specifies the amount of time the HTTP Client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.  |
| Retries          | Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.   |
| Proxy            | Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.  |

**Related Commands**

| Command                                | Description  |
|--|--|
| <b>copy</b>                            | Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system. |
| <b>debug ip http client</b>            | Enables debugging output for the HTTP client.  |
| <b>ip http client connection</b>       | Configures the HTTP client connection.   |
| <b>ip http client password</b>         | Configures a password for all HTTP client connections.   |
| <b>ip http client proxy-server</b>     | Configures an HTTP proxy server.   |
| <b>ip http client source-interface</b> | Configures a source interface for the HTTP client.   |
| <b>ip http client username</b>         | Configures a login name for all HTTP client connections.   |
| <b>show ip http client connection</b>  | Displays a report about HTTP client active connections.  |
| <b>show ip http client history</b>     | Displays the URLs accessed by the HTTP client.   |

# show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in user EXEC or privileged EXEC mode.

**show ip http server** {all| status| session-module| connection| statistics| history}

## Syntax Description

|                       |   |
|-----------------------|---|
| <b>all</b>            | Displays all HTTP server information.   |
| <b>status</b>         | Displays only HTTP server status configuration.   |
| <b>session-module</b> | Displays only supported HTTP services (Cisco IOS modules).  |
| <b>connection</b>     | Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.                         |
| <b>statistics</b>     | Displays only HTTP server connection statistics.  |
| <b>history</b>        | 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.                                    |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

## 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.

**Note**

The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

**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      192.168.254.45:33737   70         2294
HTTP server statistics:
Accepted connections total: 1360
HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
172.19.254.37:80      192.168.254.45:63530   60         1596      10:50:00 12/19
```

The table below describes the significant fields shown in the display.

**Table 5: show ip http server Field Descriptions**

| Field                              | Description   |
|------------------------------------|---|
| HTTP server status:                | Enabled or disabled. Corresponds to the <b>[no] ip http server</b> command.   |
| HTTP server port:                  | Port used by the HTTP server. Corresponds to the <b>ip http port</b> command.   |
| HTTP server authentication method: | Authentication method used for HTTP server logins. Corresponds to the <b>ip http authentication</b> 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 <b>ip http access-class</b> command. |
| HTTP server base path:             | Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the <b>ip http path</b> command.                                     |

| Field  | Description  |
|--|--|
| Maximum number of concurrent server connections allowed: | Corresponds to the <b>ip http max-connections</b> 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 <b>ip http timeout-policy</b> command.   |
| Server life time-out:                                    | The maximum number of seconds the connection will be kept open. Corresponds to the <b>ip http timeout-policy</b> 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 <b>ip http timeout-policy</b> command.   |
| 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 <b>show ip http server secure status</b> command will appear after this line.  |
| HTTP server application session modules:                 | <p>Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including:</p> <ul style="list-style-type: none"> <li>• The Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server</li> <li>• The VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM)</li> <li>• The QoS Device Manager (QDM) application, which uses the QDM Server</li> <li>• The IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS)</li> </ul> <p><b>Note</b> The IP Phone and Telephony Service applications use the ITS Local Directory Search and IOS Telephony Server (ITS). Therefore, these two applications are not supported with Cisco IOS Release 12.2(31)SB2.</p> |
| HTTP server current connections:                         | Currently active HTTP connections.   |

| Field                   | Description   |
|-------------------------|---|
| 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 (endtime). Endtime is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format:<br><br><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-ede-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  |
|--|--|
| <b>debug ip http server all</b>          | Enables debugging output for all HTTP processes on the system.               |
| <b>ip http secure-server</b>             | Enables the HTTPS server.  |
| <b>ip http server</b>                    | Enables the HTTP 1.1 server, including the Cisco web browser user interface. |
| <b>show ip http server secure status</b> | Displays the status of the HTTPS server.                                     |

# show ip http server secure status

To display the status of the HTTP secure server configuration, use the **show ip http server secure status** command in privileged EXEC mode.

**show ip http server secure status**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.2(15)T   | This command was introduced.                                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.  |

**Examples** The following is sample output from the **show ip http server secure status** command:

```
Router# show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 1025
HTTP secure server ciphersuite: rc4-128-sha rc4-128-md5
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
The table below describes the significant fields shown in the display.
```

**Table 6: show ip http server secure status Field Descriptions**

| Field                      | Description   |
|----------------------------|---|
| HTTP secure server status: | Displays the state of secure HTTP server (“Enabled” or “Disabled”). Corresponds to the configuration of the <b>ip http secure-server</b> command. |
| HTTP secure server port:   | Displays the configuration of the <b>ip http secure-port</b> command.   |



| Field                                     | Description   |
|---|---|
| HTTP secure server ciphersuite:           | Displays the configuration of the <b>ip http secure-ciphersuite</b> command.  |
| HTTP secure server client authentication: | Displays the configuration of the <b>ip http secure-client-auth</b> command.  |
| HTTP secure server trustpoint:            | Displays the configuration of the <b>ip http secure-trustpoint</b> command. If no trustpoint is configured, the line will appear blank after the colon. |

### Related Commands

| Command                           | Description   |
|-----------------------------------|---|
| <b>ip http secure-ciphersuite</b> | Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the server to a remote client. |
| <b>ip http secure-client-auth</b> | Configures the HTTP server to authenticate the remote client during the connection process.                                       |
| <b>ip http secure-port</b>        | Specifies the port (socket) to be used for HTTPS connections.   |
| <b>ip http secure-server</b>      | Enables the HTTPS server.   |
| <b>ip http secure-trustpoint</b>  | Specifies the CA trustpoint that should be used for obtaining signed certificates for the secure HTTP server.                     |

