HTTP 1.1 Web Server and Client

First Published: December 4, 2006
Last Updated: December 4, 2006

The HTTP 1.1 Web Server and Client feature provides a consistent interface for users and applications by implementing support for HTTP 1.1 in Cisco IOS software-based devices. The integrated HTTP server application program interface (API) supports server application interfaces and provides a complete solution for HTTP services to and from Cisco devices.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for the HTTP 1.1 Web Server and Client" section on page 67.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for HTTP 1.1 Web Server and Client

The secure HTTP (HTTPS) server and client—secure HTTP communication in which Secure Socket Layer (SSL) encryption technology provides HTTP server and client authentication and is used to encrypt data sent to and received from an HTTP server—are not supported in the HTTP 1.1 web server and client feature in Cisco IOS Release 12.2(31)SB2.

Information About the HTTP 1.1 Web Server and Client

To use the HTTP 1.1 web server and client, you should understand the following concepts:

HTTP 1.1 with Cisco Devices

This feature updates the Cisco implementation of HTTP from 1.0 to 1.1. The HTTP server allows features and applications, such as the Cisco web browser user interface, to be run on your routing device.

The Cisco implementation of HTTP 1.1 is backward compatible with previous Cisco IOS releases. If you are currently using configurations that enable the HTTP server, no configuration changes are needed, as all defaults remain the same.

The process of enabling and configuring the HTTP server also remains the same as in previous releases. Support for Server Side Includes (SSI) and HTML forms has not changed. Additional configuration options, in the form of the **ip http timeout-policy** command and the **ip http max-connections** command have been added. These options allow configurable resource limits for the HTTP server. If you do not use these optional commands, the default policies are used.

Remote applications may require that you enable the HTTP server before using them. Applications that use the HTTP server include the following:

- Cisco web browser user interface—This user interface uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server.
- VPN Device Manager (VDM) application—VDM uses the VDM Server and the XML Session Manager (XSM).
- QoS Device Manager (QDM) application—QDM uses the QDM Server.

HTTP Server General Access Policies

General access characteristics for the server can be specified using the **ip http timeout-policy** command to configure a value for idle time, connection life, and request maximum. By adjusting these values you can configure a general policy; for example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can configure such a policy by specifying large values for the **life** and **request** options so that each connection stays open longer and more requests are processed for each connection.

Another example is to configure a policy that minimizes the response time for new connections by specifying small values for the **life** and **request** options so that the connections are quickly released to serve new clients.

A throughput policy is better for HTTP sessions with dedicated management applications, because it allows the application to send more requests before the connection is closed, while a response time policy is better for interactive HTTP sessions, because it allows more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Access security policies for the HTTP server are configured using the **ip http authentication** command, which allows only selective users to access the server, and the **ip http access-class** command, which allows only selective IP hosts to access the server.

Selective Enabling of Applications Within the HTTP Infrastructure

The ability to selectively enable applications using an HTTP server feature eliminates a potential security vulnerability by providing a facility to enable selected HTTP services on the Cisco IOS HTTP server infrastructure. This feature also provides the capability to view the current state of the HTTP services, including which services are enabled or disabled.

Prior to this feature, HTTP applications running on a router or a switch were either all enabled or all disabled when the HTTP server was enabled or disabled using the **ip http server** command. In the situation where all HTTP applications were enabled, remote end-users were given potential access to services that could allow remote end-users to pose a potential security threat to service providers.

With ability to selectively enable applications using an HTTP server, the Cisco IOS HTTP infrastructure provides a way to enable only selected HTTP applications to run on a router or a switch, thereby bypassing a potential security vulnerability. Selected HTTP applications can be enabled using the **ip http active-session-modules** configuration command.

Note The maximum number of sessions that can be registered with the Cisco IOS HTTP server is 32.

How to Configure the HTTP 1.1 Web Server and Client

This section contains the following tasks:

Enabling and Configuring the HTTP Server

To enable the HTTP server and configure optional server characteristics, perform the following steps. The HTTP server is disabled by default.

Restrictions

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http authentication** {**aaa** {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**}
5. **ip http port** *port-number*
6. **ip http path** *url*
7. **ip http access-class** *access-list-number*
8. **ip http max-connections** *value*
9. **ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

	Command or Action	Purpose
Step 4	**ip http authentication** {**aaa** {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**} **Example:** `Router(config)# ip http authentication aaa login-authentication LOCALDB`	(Optional) Specifies the authentication method to be used for login when a client connects to the HTTP server. The authentication method settings are as follows: • Whether the authentication method used for the AAA login service (specified by the **aaa authentication login default** command) should be used for authentication. • Whether the "enable" password should be used for authentication. (This is the default method.) • Whether the login username, password, and privilege level access combination specified in the local system configuration (by the **username global configuration** command) should be used for authentication and authorization. • Whether the TACACS (or XTACACS) server should be used for authentication.
Step 5	**ip http port** *port-number* **Example:** `Router(config)# ip http port 8080`	(Optional) Specifies the server port that should be used for HTTP communication (for example, for the Cisco web browser user interface).
Step 6	**ip http path** *url* **Example:** `Router(config)# ip http path slot1:`	(Optional) Sets the base HTTP path for HTML files. The base path is used to specify the location of the HTTP server files (HTML files) on the local system. Generally, the HTML files are located in system flash memory.
Step 7	**ip http access-class** *access-list-number* **Example:** `Router(config)# ip http access-class 20`	(Optional) Specifies the access list that should be used to allow access to the HTTP server.
Step 8	**ip http max-connections** *value* **Example:** `Router(config)# ip http max-connections 10`	(Optional) Sets the maximum number of concurrent connections to the HTTP sever that will be allowed. The default value is 5.
Step 9	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value* **Example:** `Router(config)# ip http timeout-policy idle 30 life 120 requests 100`	(Optional) Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are as follows: • The maximum number of seconds the connection will be kept open if no data is received or response data can not be sent out on the connection. • The maximum number of seconds the connection will be kept open, from the time the connection is established. • The maximum limit on the number of requests processed on a persistent connection before it is closed.

Enabling Selected HTTP Applications

Perform this task to selectively enable the HTTP applications that will service incoming HTTP requests from remote clients.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http session-module-list** *listname prefix1* [*prefix2,..., prefixn*]
4. **ip http active-session-modules** {*listname* | **none** | **all**}
5. **end**
6. **show ip http server session-module**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http session-module-list** *listname prefix1* [*prefix2,...,prefixn*] **Example:** `Router(config)# ip http session-module-list list1 SCEP,HOME_PAGE`	Defines a list of HTTP application names.
Step 4	**ip http active-session-modules** {*listname* | **none** | **all**} **Example:** `Router(config)# ip http active-session-modules list1`	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients. The applications can be enabled using one of the following criteria: • Only those HTTP services configured in the list identified by the **ip http session-module-list** command are enabled to serve HTTP requests. • All HTTP services are disabled from serving HTTP requests. • All HTTP services are enabled to serve HTTP requests.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Ends your configuration session and returns the CLI to privileged EXEC mode.
Step 6	**show ip http server session-module** **Example:** `Router# show ip http server session-module`	(Optional) Displays information about all HTTP services available on the router or switch, including their current state of service, such as whether they are enabled or disabled.

Configuring the HTTP Client Default Username and Password

The standard HTTP 1.1 client is always enabled and there are no commands that exist to disable the HTTP client. Commands are available that can be used to set the default username and password for all connection requests with the remote HTTP server. To set the default username and password, perform the following steps.

Restrictions

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http client username** *username*
4. **ip http client password** *password*
5. **do copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http client username** *username* **Example:** `Router(config)# ip http client username User1`	Configures the default username used for connections to remote HTTP servers.

	Command or Action	Purpose
Step 4	**ip http client password** *password* **Example:** `Router(config)# ip http client password Secret`	Configures the default password used for connections to remote HTTP servers.
Step 5	**do copy running-config startup-config** **Example:** `Router(config)# do copy running-config startup-config`	(Optional) Saves the running configuration as the startup configuration file. • The **do** command allows you to execute EXEC mode commands from global configuration mode.

Configuring Other HTTP Client Connection Characteristics and Cache

The standard HTTP 1.1 client is always enabled and there are no commands that exist to disable the HTTP client. There are a number of optional characteristics that can be configured for the standard HTTP client. Perform this task to configure optional characteristics of the HTTP client. One or more of the following steps can be performed in any order.

Restrictions

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip http client connection** {**forceclose** | **idle timeout** *seconds* | **retry** *count* | **timeout** *seconds*} **Example:** `Router(config)# ip http client connection idle timeout 15`	(Optional) Configures characteristics for HTTP client connections to a remote HTTP server.
Step 4	**ip http client proxy-server** {*proxy-name* | *ip-address*} [**proxy-port** *port-number*] **Example:** `Router(config)# ip http client proxy-server edge2 proxy-port 29`	(Optional) Configures the HTTP client to connect to a remote proxy server for HTTP file system client connections. • The optional **proxy-port** *port-number* syntax allows you to specify the proxy port number on the remote proxy server.
Step 5	**ip http client response timeout** *seconds* **Example:** `Router(config)# ip http client response timeout 180`	(Optional) Specifies the number of seconds the HTTP client waits for a response from the server for a request message before giving up.
Step 6	**ip http client source-interface** *interface-id* **Example:** `Router(config)# ip http client source-interface Ethernet 0/1`	(Optional) Specifies the interface for source address in all HTTP client connections.
Step 7	**ip http client cache** {**ager** *interval minutes* | **memory file** *file-size-limit* | **memory pool** *pool-size-limit*} **Example:** `Router(config)# ip http client cache ager interval 10`	(Optional) Configures the HTTP client cache ager interval, maximum file size, or maximum memory pool size.

Configuration Examples for the HTTP 1.1 Web Server and Client

This section provides the following configuration examples:

- HTTP Server Enabling and Configuration: Example, page 10
- HTTP Connectivity Verification: Example, page 10
- HTTP Applications Enabled Selectively: Example, page 10

HTTP Server Enabling and Configuration: Example

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

```
Router(config)# ip http server
Router(config)# ip http authentication aaa
Router(config)# ip http path flash:
Router(config)# ip http access-class 10
Router(config)# ip http max-connections 10
```

In the following example, a Throughput timeout policy is applied. This configuration allows each connection to be idle a maximum of 30 seconds (approximately). Each connection will remain open (be "alive") until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately100 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 allows each connection to be idle a maximum of 30 seconds (approximately). Each connection will be closed when the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

HTTP Connectivity Verification: Example

To verify remote connectivity to the HTTP server, enter the system IP address in a web browser, followed by a colon and the appropriate port number (80 is the default port number).

For example, if the system IP address is 209.165.202.129 and the port number is 8080, enter **http://209.165.202.129:8080** as the URL in a web browser.

If HTTP authentication is configured, a login dialog box will appear. Enter the appropriate username and password. If the default login authentication method of "enable" is configured, you may leave the username field blank, and use the "enable" password to log in.

The system home page should appear in your browser.

HTTP Applications Enabled Selectively: Example

The following configuration sample shows a configuration with different set of services available for HTTP requests. In this example, only the HTTP applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE and HTTP IFS) are enabled for providing services to remote HTTP clients.

```
ip http session-module-list list1 HOME_PAGE,HTTP_IFS
ip http active-session-modules list1
ip http server
```

Additional References

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

Related Documents

Related Topic	Document Title
Additional HTTP configuration information	"Using the Cisco Web Browser User Interface" chapter in the section "Cisco IOS User Interfaces" in the *Cisco IOS Configuration Fundamentals Guide*, Release 12.2.
Additional HTTP commands	*Cisco IOS Network Management Command Reference*, Release 12.2(31)SB2.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. **Note** HTTP 1.1, as defined in RFC 2616, is currently classified as a "Standards Track" document by the IETF.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2616 The Cisco implementation of the HTTP version 1.1 supports a subset of elements defined in RFC 2616. The following is a list of supported RFC 2616 headers: • Allow (Only GET, HEAD, and POST methods are supported) • Authorization, WWW-Authenticate - Basic authentication only • Cache-control • Chunked Transfer Encoding • Connection close • Content-Encoding • Content-Language • Content-Length • Content-Type • Date, Expires • Location	"Hypertext Transfer Protocol -- HTTP/1.1"

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- **clear ip http client cache**

Modified Commands

- **debug ip http all**
- **debug ip http authentication**
- **debug ip http client**

- debug ip http ezsetup
- debug ip http ssi
- debug ip http token
- debug ip http transaction
- debug ip http url
- ip http access-class
- ip http active-session-modules
- ip http authentication
- ip http client cache
- ip http client connection
- ip http client password
- ip http client proxy-server
- ip http client response
- ip http client source-interface
- ip http client username
- ip http max-connections
- ip http path
- ip http port
- ip http server
- ip http session-module-list
- ip http timeout-policy
- show ip http client
- show ip http server

clear ip http client cache

To remove information from the HTTP client cache, use the **clear ip http client cache** command in privileged EXEC mode.

clear ip http client cache {**all** | **session** *session-name* | **url** *complete-url*}

Syntax Description

cache all	Removes all HTTP client cache entries.
cache session *session-name*	Removes HTTP client cache entries of the HTTP client application session specified by the *session-name* argument.
cache url *complete-url*	Removes the HTTP client cache entry whose location is specified by the *complete-url* argument, a Cisco IOS File System (IFS) Uniform Resource Locator (URL), and that consists of HTML files used by an HTTP server.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

Use this command to clear entries from the HTTP client cache pool: all the entries, all the entries owned by a specific session, or only the entry associated with a specific request from an HTTP server.

Examples

The following example clears all entries in the HTTP client cache:

```
Router# clear ip http client cache all
```

The following example removes HTTP client cache entries that belong to the HTTP Client File System (CFS) application:

```
Router# clear ip http client cache session HTTP CFS
```

The following example removes HTTP client cache entries at the location http://myrouter.cisco.com/flash:/:

```
Router# clear ip http client cache url http://myrouter.cisco.com/flash:/
```

Related Commands

Command	Description
ip http path	Specifies the base path used to locate files for use by the HTTP server.
show ip http client	Displays a report about the HTTP client.

debug ip http all

To enable debugging output for all HTTP processes on the system, use the **debug ip http all** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http all

no debug ip http all

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

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.

Usage Guidelines

Use this command to enable debugging messages for all HTTP processes and activity. Issuing this command is equivalent to issuing the following commands:

- **debug ip http authentication**
- **debug ip http ezsetup**
- **debug ip http ssi**
- **debug ip http token**
- **debug ip http transaction**
- **debug ip http url**

Examples

For sample output and field descriptions of this command, see the documentation of the commands listed in the "Usage Guidelines" section.

Related Commands

Command	Description
debug ip http authentication	Enables debugging output for all processes for HTTP server and client access.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.

Command	Description
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed from the router.

debug ip http authentication

To troubleshoot HTTP authentication problems, use the **debug ip http authentication** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http authentication

no debug ip http authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

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.

Usage Guidelines

Use this command to display the authentication method the router attempted and authentication-specific status messages.

Examples

The following is sample output from the **debug ip http authentication** command:

```
Router# debug ip http authentication

Authentication for url '/' '/' level 15 privless '/'
Authentication username = 'local15' priv-level = 15 auth-type = local
```

Table 1 describes the significant fields shown in the display.

Table 1 debug ip http authentication Field Descriptions

Field	Description
Authentication for url	Provides information about the URL in different forms.
Authentication username	Identifies the user.
priv-level	Indicates the user privilege level.
auth-type	Indicates the authentication method.

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.

Command	Description
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed from the router.

debug ip http client

To enable debugging output for the HTTP client, use the **debug ip http client** command in privileged EXEC mode. To disable debugging output for the HTTP client, use the **no** or **undebug** form of this command.

debug ip http client {**all** | **api** | **cache** | **error** | **main** | **msg** | **socket**}

no debug ip http client {**all** | **api** | **cache** | **error** | **main** | **msg** | **socket**}

undebug ip http client {**all** | **api** | **cache** | **error** | **main** | **msg** | **socket**}

Syntax Description

all	Enables debugging for all HTTP client elements.
api	Enables debugging output for the HTTP client application interface (API).
cache	Enables debugging output for the HTTP client cache.
error	Enables debugging output for HTTP communication errors.
main	Enables debugging output specific to the Voice XML (VXML) applications interacting with the HTTP client.
msg	Enables debugging output of HTTP client messages.
socket	Enables debugging output specific to the HTTP client socket.

Command Modes

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.

Usage Guidelines

Use this command to display transactional information for the HTTP client for debugging purposes.

Examples

The following example shows sample debugging output for a failed **copy** transfer operation when the host name resolution fails:

```
Router# debug ip http client all

2w4d: Cache ager called
Router# copy http://www.example.com/index.html flash:index.html
Destination filename [index.html]?
Erase flash: before copying? [confirm] no
Translating "www.example.com"

% Bad IP address for host www.example.com
%Error opening http://www.example.com/index.html (I/O error)
Router#

2w4d: http_client_request:
```

```
2w4d: httpc_setup_request:

2w4d: http_client_process_request:

2w4d: HTTPC: Host name resolution failed for www.example.com

2w4d: http_transaction_free:

2w4d: http_transaction_free: freed httpc_transaction_t
```

The following example shows sample debugging output for a failed **copy** transfer operation when the source file is not available:

```
Router# copy http://example.com/hi/file.html flash:/file.html
Destination filename [file.html]?
%Error opening http://example.com/hi/file.html (No such file or directory)
Router#
2w4d: http_client_request:

2w4d: httpc_setup_request:

2w4d: http_client_process_request:
2w4d: httpc_request:Dont have the credentials

Thu, 17 Jul 2003 07:05:25 GMT  http://209.168.200.225/hi/file.html ok
        Protocol = HTTP/1.1
        Content-Type = text/html; charset=iso-8859-1
        Date = Thu, 17 Jul 2003 14:24:29 GMT

2w4d: http_transaction_free:

2w4d: http_transaction_free:freed httpc_transaction_t

2w4d: http_client_abort_request:
2w4d: http_client_abort_request:Bad Transaction Id
Router#
```

Table 2 describes the significant fields shown in the display.

Table 2 debug ip http client Field Descriptions

Field	Description
2w4d:	In the examples shown, the string "2w4d" is the timestamp configured on the system. Indicates two weeks and four days since the last system reboot. • The time stamp format is configured using the **service timestamps debug** global configuration mode command.
HTTPC: or httpc	Indicates the HTTP client in Cisco IOS software.

Table 2 debug ip http client Field Descriptions (continued)

Field	Description
httpc_request:Dont have the credentials	Indicates that this HTTP client request did not supply any authentication information to the server. The authentication information consists of a username and password combination. The message is applicable to both HTTP and HTTPS.
Thu, 17 Jul 2003 07:05:25 GMT http://209.168.200.225/hi/file.html ok	The "ok" in this line indicates that there were no internal errors relating to processing this HTTP client transaction by the HTTP client. In other words, the HTTP client was able to send the request and receive some response. **Note** The "ok" value in this line does not indicate file availability ("200: OK" message or "404: File Not Found" message).

Related Commands

Command	Description
copy	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.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
service timestamps	Configures the time-stamping format for debugging or system logging messages.
show ip http client connection	Displays a report about HTTP client active connections.
show ip http client history	Displays the URLs accessed by the HTTP client.
show ip http client session-module	Displays a report about sessions that have registered with the HTTP client.

debug ip http ezsetup

To display the configuration changes that occur during the EZ Setup process, use the **debug ip http ezsetup** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http ezsetup

no debug ip http ezsetup

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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use this command to verify the EZ Setup actions without changing the configuration of the router.

EZ Setup is a form you fill out to perform basic router configuration from most HTML browsers.

Examples

The following sample output from the **debug ip http ezsetup** command shows the configuration changes for the router when the EZ Setup form has been submitted:

```
Router# debug ip http ezsetup

service timestamps debug
service timestamps log
service password-encryption
!
hostname router-name
!
enable secret router-pw
line vty 0 4
password router-pw
!
interface ethernet 0
 ip address 172.69.52.9 255.255.255.0
 no shutdown
 ip helper-address 172.31.2.132
ip name-server 172.31.2.132
isdn switch-type basic-5ess
username Remote-name password Remote-chap
interface bri 0
 ip unnumbered ethernet 0
 encapsulation ppp
 no shutdown
 dialer map ip 192.168.254.254 speed 56 name Remote-name Remote-number
 isdn spid1 spid1
```

```
 isdn spid2 spid2
 ppp authentication chap callin
 dialer-group 1
!
ip classless
access-list 101 deny udp any any eq snmp
access-list 101 deny udp any any eq ntp
access-list 101 permit ip any any
dialer-list 1 list 101
ip route 0.0.0.0 0.0.0.0 192.168.254.254
ip route 192.168.254.254 255.255.255.255 bri 0
logging buffered
snmp-server community public RO
ip http server
ip classless
ip subnet-zero
!
end
```

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http authentication	Displays authentication processes for HTTP server and client access.
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed from the router.

debug ip http ssi

To display information about the HTML SSI EXEC command or HTML SSI ECHO command, use the **debug ip http ssi** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http ssi

no debug ip http ssi

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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following is sample output from the **debug ip http ssi** command:

```
Router# debug ip http ssi

HTML: filtered command ‘exec cmd="show users"’
HTML: SSI command ‘exec’
HTML: SSI tag ‘cmd’ = "show users"
HTML: Executing CLI ‘show users’ in mode ‘exec’ done
```

The following line shows the contents of the SSI EXEC command:

```
HTML: filtered command ‘exec cmd="show users"’
```

The following line indicates the type of SSI command that was requested:

```
HTML: SSI command ‘exec’
```

The following line shows the *show users* argument assigned to the **tag** command:

```
HTML: SSI tag ’cmd’ = "show users"
```

The following line indicates that the **show users** command is being executed in EXEC mode:

```
HTML: Executing CLI ‘show users’ in mode ‘exec’ done
```

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http authentication	Displays authentication processes for HTTP server and client access.

Command	Description
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed from the router.

debug ip http token

To display individual tokens parsed by the HTTP server, use the **debug ip http token** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http token

no debug ip http token

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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **debug ip http token** command to display low-level HTTP server parsings. To display high-level HTTP server parsings, use the **debug ip http transaction** command.

Examples

The following is part of sample output from the **debug ip http token** command. In this example, the browser accessed the router's home page http://router-name/. The output gives the token parsed by the HTTP server and its length.

```
Router# debug ip http token

HTTP: token len 3: 'GET'
HTTP: token len 1: ' '
HTTP: token len 1: '/'
HTTP: token len 1: ' '
HTTP: token len 4: 'HTTP'
HTTP: token len 1: '/'
HTTP: token len 1: '1'
HTTP: token len 1: '.'
HTTP: token len 1: '0'
HTTP: token len 2: '\15\12'
HTTP: token len 7: 'Referer'
HTTP: token len 1: ':'
HTTP: token len 1: ' '
HTTP: token len 4: 'http'
HTTP: token len 1: ':'
HTTP: token len 1: '/'
HTTP: token len 1: '/'
HTTP: token len 3: 'www'
HTTP: token len 1: '.'
HTTP: token len 3: 'thesite'
HTTP: token len 1: '.'
HTTP: token len 3: 'com'
HTTP: token len 1: '/'
```

```
HTTP: token len 2: '\15\12'
HTTP: token len 10: 'Connection'
HTTP: token len 1: ':'
HTTP: token len 1: ' '
HTTP: token len 4: 'Keep'
HTTP: token len 1: '-'
HTTP: token len 5: 'Alive'
HTTP: token len 2: '\15\12'
HTTP: token len 4: 'User'
HTTP: token len 1: '-'
HTTP: token len 5: 'Agent'
HTTP: token len 1: ':'
HTTP: token len 1: ' '
HTTP: token len 7: 'Mozilla'
HTTP: token len 1: '/'
HTTP: token len 1: '2'
HTTP: token len 1: '.'
.
.
.
```

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http authentication	Displays authentication processes for HTTP server and client access.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.
debug ip http transaction	Displays HTTP server transaction processing.
debug ip http url	Displays the URLs accessed from the router.

debug ip http transaction

To display HTTP server transaction processing, use the **debug ip http transaction** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http transaction

no debug ip http transaction

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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **debug ip http transaction** command to display what the HTTP server is parsing at a high level. To display what the HTTP server is parsing at a low level, use the **debug ip http token** command.

Examples

The following is sample output from the **debug ip http transaction** command. In this example, the browser accessed the router's home page http://router-name/.

```
Router# debug ip http transaction

HTTP: parsed uri '/'
HTTP: client version 1.1
HTTP: parsed extension Referer
HTTP: parsed line http://www.company.com/
HTTP: parsed extension Connection
HTTP: parsed line Keep-Alive
HTTP: parsed extension User-Agent
HTTP: parsed line Mozilla/2.01 (X11; I; FreeBSD 2.1.0-RELEASE i386)
HTTP: parsed extension Host
HTTP: parsed line router-name
HTTP: parsed extension Accept
HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
HTTP: parsed extension Authorization
HTTP: parsed authorization type Basic
HTTP: received GET ''
```

Table 3 describes the significant fields shown in the display.

Table 3 debug ip http transaction Field Descriptions

Field	Description
HTTP: parsed uri '/'	Uniform resource identifier that is requested.
HTTP: client version 1.1	Client HTTP version.
HTTP: parsed extension Referer	HTTP extension.
HTTP: parsed line http://www.company.com/	Value of HTTP extension.
HTTP: received GET ''	HTTP request method.

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http authentication	Displays authentication processes for HTTP server and client access.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.
debug ip http url	Displays the URLs accessed from the router.

debug ip http url

To show the URLs accessed from the router, use the **debug ip http url** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip http url

no debug ip http url

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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **debug ip http url** command to keep track of the URLs that are accessed and to determine from which hosts the URLs are accessed.

Examples

The following is sample output from the **debug ip http url** command. In this example, the HTTP server accessed the URLs and /exec. The output shows the URL being requested and the IP address of the host requesting the URL.

```
Router# debug ip http url

HTTP: processing URL '/' from host 172.31.2.141
HTTP: processing URL '/exec' from host 172.31.2.141
```

Related Commands

Command	Description
debug ip http all	Displays authentication processes for all HTTP server processes on the system.
debug ip http authentication	Displays authentication processes for HTTP server and client access.
debug ip http ezsetup	Displays the configuration changes that occur during the EZ Setup process.
debug ip http ssi	Displays SSI translations and SSI ECHO command execution.
debug ip http token	Displays individual tokens parsed by the HTTP server.
debug ip http transaction	Displays HTTP server transaction processing.

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

access-list-number	Standard IP access list number in the range 0 to 99, as configured by the **access-list** global configuration command.

Command Default

No access list is applied to the HTTP server.

Command Modes

Global configuration

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.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

In the following example the access list identified as “20” is defined and assigned to the HTTP server:

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.130 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
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command in global configuration mode. Use the **no** form of this command to return to the default, for which all HTTP services will be enabled.

ip http active-session-modules {*listname* | **none** | **all**}

no ip http active-session-modules {*listname*}

Syntax Description

listname	Enables only those HTTP services configured in the list identified by the **ip http session-module-list** command to serve HTTP requests. All other HTTP or HTTPS applications on the router or switch will be disabled.
none	Disables all HTTP services.
all	Enables all HTTP applications to service incoming HTTP requests from remote clients.

Defaults

If no arguments or keywords are specified, all HTTP services will be enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or secure HTTP (HTTPS) application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

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

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
```

```
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
ip http session-module-list	Defines a list of HTTP or HTTPS application names.
show ip http server	Displays details about the current configuration of 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

aaa	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 **aaa authentication login default** command, unless otherwise specified by the **login-authentication** *listname* keyword and argument.
command-authorization	Sets the authorization method list for commands at the specified privilege level.
level	Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router: • 0—Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands. • 1—Includes all user-level commands at the router prompt (>). • 15—Includes all enable-level commands at the router prompt (>).
listname	Sets the name of the method list.
exec-authorization	Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session.
login-authentication	Sets the method list for login authentication, which enables AAA authentication for logins.
enable	Indicates that the "enable" password should be used for authentication. (This is the default method.)
local	Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.
tacacs	Indicates that the TACACS (or XTACACS) server should be used for authentication.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.3(8)T	The **tacacs** keyword was removed. The **command-authorization**, **exec-authorization**, and **login-authentication** 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 **ip http authentication aaa** command option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

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

Note When the "enable" password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the "enable" password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only "enable" password for authentication is strongly discouraged. Instead, use of the **local** or **tacacs** authentication options, configured as part of a global AAA framework, is recommended.
To configure HTTP access as part of a AAA policy, use the **ip http authentication aaa** command option. The "local", "tacacs", or "enable" authentication methods should then be configured using the **aaa authentication login** command.

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

Examples

The following example specifies that the method configured for AAA should be used for authentication for HTTP server users. The AAA login method is configured as the "local" username/password authentication method. This example specifies that the local username database be used 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
aaa authentication login	Specifies the login authentication method to be used by the AAA service.
aaa authorization	Sets parameters that restrict user access to a network.
ip http server	Enables the HTTP server.

ip http client cache

To configure the HTTP client cache, use the **ip http client cache** command in global configuration mode. To remove the specification of a value configured for the HTTP client cache, use the **no** form of this command.

ip http client cache {**ager interval** *minutes* | **memory file** *file-size-limit* | **memory pool** *pool-size-limit*}

no ip http client cache {**ager interval** | **memory file** | **memory pool**}

Syntax Description

ager interval *minutes*	The *minutes* argument specifies the frequency, in minutes, at which the router removes expired cached responses from the HTTP client cache pool. The range is from 0 to 60, and the default is 5. **Note** The explicit expiration time for a cached response can be provided by the origin server. If this information is not configured, the HTTP cache uses heuristic calculations to determine a plausible expiration time for the cached response.
memory file *file-size-limit*	The *file-size-limit* argument specifies the maximum file size, in kilobytes, supported by the HTTP client cache. The range is from 1 to10, and the default is 2.
memory pool *pool-size-limit*	The *pool-size-limit* argument specifies the maximum memory pool size, in kilobytes, allowed for the HTTP client cache. The range is from 0 to 100, and the default is 100.

Command Default

5 second ager interval for the HTTP client cache memory pool
2 KB maximum file size supported by the HTTP client cache
100 KB maximum memory pool size for the HTTP client cache

Command Modes

Global configuration.

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.

Usage Guidelines

Use this command to specify the HTTP client cache ager interval, maximum file size, or maximum memory pool size.

To display the values configured by this command, use the **show ip http client cache** command.

Examples

The following example specifies an HTTP client cache ager interval of 10 minutes:

```
Router(config)# ip http client cache ager interval 10
```

The following example specifies an HTTP client cache maximum file size of 7 KB:

```
Router(config)# ip http client cache memory file 7
```

The following example specifies an HTTP client cache maximum memory pool size of 55 KB:

```
Router(config)# ip http client cache memory pool 55
```

Related Commands

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

ip http client connection

To configures characteristics for HTTP client connections to a remote HTTP server for all file transfers, use the **ip http client connection** command in global configuration mode. To remove the specification of a value configured for a connection characteristic, use the **no** form of this command.

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

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

Syntax Description

forceclose	Disables a persistent connection. Enabled by default.
idle timeout *seconds*	Sets the period of time allowed for an idle connection between an HTTP client and server before the connection is closed. Accepted range is from 1 to 60 seconds. Default period is 30 seconds.
retry *count*	Sets the in case of connection establishment timeout. Accepted range is from 1 to 5 retries. Default count is 1 retry.
timeout *seconds*	Sets the maximum time the HTTP client will wait for a connection. Accepted range is from 1 to 60 seconds. Default is 10 seconds.

Defaults

Persistent connection maintenance is enabled.
30-second idle timeout
1 retry attempt
10-second maximum timeout

Command Modes

Global configuration

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.

Usage Guidelines

Use this command to change or remove the specification of a value configured as a characteristics for establishing an HTTP client connection to a remove HTTP server for all file transfers.

Examples

The following example configures the default HTTP client persistent connection for a 15-second idle connection period. The maximum time the HTTP client will wait for a connection is 10 seconds.

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

Related Commands

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

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 *password*

no ip http client password

Syntax Description

password	The password string to be used in HTTP client connection requests sent to remote HTTP servers.

Defaults

No default password exists for the HTTP connections.

Command Modes

Global configuration

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.

Usage Guidelines

This command is used to configure a default password before a file is download 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 Secret and the default HTTP username is configured as User2 for connections to remote HTTP or HTTPS servers:

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

Related Commands

Command	Description
copy	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.
debug ip http client	Enables debugging output for the HTTP client.

Command	Description
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	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* | *ip-address*} [**proxy-port** *port-number*]

no ip http client proxy-server

Syntax Description

proxy-name | *ip-address*	Name or IP address for the proxy server.
proxy-port *port-number*	(Optional) Specifies a port number on the remote proxy server.

Defaults

No default behavior or values

Command Modes

Global configuration

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.

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 configures the HTTP proxy server named edge2 at port 29:

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

Related Commands

Command	Description
copy	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.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.

Command	Description
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	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 specification of the number of seconds that the HTTP client waits for a response from the server for a request message, use the **no** form of this command.

ip http client response timeout *seconds*

no ip http client response timeout

Syntax Description

timeout *seconds*	The *seconds* argument specifies the 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

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.

Usage Guidelines

Use this command to specify the response timeout value.

Examples

The following example specifies a response timeout of 180 seconds:

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

Related Commands

Command	Description
copy	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.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.

Command	Description
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

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 *interface-id*

no ip http client source-interface

Syntax Description

interface-id	Name and number of the source interface.

Defaults

No default behavior or values

Command Modes

Global configuration

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.

Usage Guidelines

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

Examples

The following example configures the source interface as Ethernet 0/1:

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

Related Commands

Command	Description
copy	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.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.

Command	Description
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	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

username	The username string (login name) to be used in HTTP client connection requests sent to remote HTTP servers.

Defaults

No default username exists for the HTTP connections.

Command Modes

Global configuration

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.

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
copy	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.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.

Command	Description
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
show ip http client	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

value	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

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.

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 any new connections until the current number of connections falls below the new configured value.

Examples

In the following example the HTTP server is configured to allow up to 10 simultaneous connections:

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

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http path

To specify the base path used to locate files for use by the HTTP server, use the **ip http path** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http path *url*

no ip http path

Syntax Description

url	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

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.

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 pathnames (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
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

ip http port

To specify the port number to be used by the HTTP server, use the **ip http port** command in global configuration mode. To return the port number to the default, use the **no** form of this command.

ip http port *port-number*

no ip http port

Syntax Description

port-number	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

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.

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

In the following example the HTTP server port is changed to port 8080:

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

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http 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

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.

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 your system at the same time. If you enable the secure HTTP 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
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the secure HTTP server.

ip http session-module-list

To define a list of HTTP or secure HTTP (HTTPS) application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

ip http session-module-list *listname prefix1* [*prefix2,...,prefixn*]

no ip http session-module-list *listname prefix1* [*prefix2,...,prefixn*]

Syntax Description

listname	Name of the list.
prefix1	Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE.
prefix2,...,prefixn	(Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma.

Defaults

No list of HTTP or HTTPS application names is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a router or switch. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

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

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http active-session-modules	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
show ip http server	Displays details about the current configuration of the HTTP server.

ip http timeout-policy

To configure the parameters for closing connections to the local HTTP server, use the **ip http timeout-policy** command in global configuration mode. To return the parameters to their defaults, use the **no** form of this command.

ip http timeout-policy idle *seconds* **life** *seconds* **requests** *value*

no ip http timeout-policy

Syntax Description

idle	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 **idle** keyword, an integer in the range from 1 to 600 seconds (10 minutes). The default is 180 seconds (3 minutes). When used with the **life** keyword, an integer in the range from 1 to 86400 seconds (24 hours). The default is 180 seconds (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

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.

Usage Guidelines

This command sets the characteristics that determine how long a connection to the HTTP server should remain open.

This command may not take effect immediately on any HTTP connections that are open at the time you use this command. In other words, new values for idle time, life time, and maximum requests will apply only to connections made to the HTTP server after this command is issued.

A connection may be closed sooner than the configured **idle** time if the server is too busy or the limit on the **life** time or the number of **requests** is reached.

A connection may be closed sooner than the configured **life** time if the server is too busy or the limit on the **idle** time or the number of **requests** is reached. Also, since the server will not close a connection while actively processing a request, the connection may remain open longer than the specified **life** time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes.

A connection may be closed before the maximum number of requests are processed if the server is too busy or the limit on the **idle** time or **life** time is reached.

The **ip http timeout-policy** command allows you to specify a general access policy to the HTTP server by adjusting the connection timeout values. For example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **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 a maximum of 30 seconds (approximately). Each connection will remain open (be "alive") until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

show ip http 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

all	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.
cache	Displays a list of information about the HTTP client cache.
connection	Displays HTTP client active connections and configured values for connections.
history	Displays a list of up to 20 URLs most recently accessed by the HTTP client.
secure status	Displays the status of the secure HTTP client configuration. **Note** This keyword is not supported with Cisco IOS Release 12.2(31)SB2.
session-module	Displays a report about sessions or applications that have registered with the HTTP client.
statistics	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 **all**, **cache**, and **statistics** keywords were added.

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
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip http client secure status Field Descriptions

Field	Description
HTTP secure client ciphersuite:	Displays the configuration of the **ip http client secure-ciphersuite** command.
HTTP secure client trustpoint:	Displays the configuration of the **ip http client secure-trustpoint** 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            :
```

Table 5 describes the fields shown in the display.

Table 5 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.
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
copy	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.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.

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

all	Displays all HTTP server information.
status	Displays only HTTP server status configuration.
session-module	Displays only supported HTTP services (Cisco IOS modules).
connection	Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.
statistics	Displays only HTTP server connection statistics.
history	Displays only the previous 20 connections to the HTTP server, including the IP address accessed, and the time when the connection was closed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip http server Field Descriptions

Field	Description
HTTP server status:	Enabled or disabled. Corresponds to the [**no**] **ip http server** command.
HTTP server port:	Port used by the HTTP server. Corresponds to the **ip http port** command.
HTTP server authentication method:	Authentication method used for HTTP server logins. Corresponds to the **ip http authentication** command.
HTTP server access class:	Access list number assigned to the HTTP server. A value of zero (0) indicates no access list is assigned. Corresponds to the **ip http access-class** command.
HTTP server base path:	Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the **ip http path** command.
Maximum number of concurrent server connections allowed:	Corresponds to the **ip http max-connections** command.
Server idle time-out:	The maximum number of seconds the connection will be kept open if no data is received or if response data can not be sent out. Corresponds to the **ip http timeout-policy** command.
Server life time-out:	The maximum number of seconds the connection will be kept open. Corresponds to the **ip http timeout-policy** command.
Maximum number of requests allowed on a connection:	The maximum number of requests that will be processed on a connection before the connection is closed. Corresponds to the **ip http timeout-policy** command.
HTTP secure server capability:	Indicates if the running software image supports the secure HTTP server (“Present” or “Not Present”). If the capability is present, the output from the **show ip http server secure status** command will appear after this line.

Table 6 show ip http server Field Descriptions (continued)

Field	Description
HTTP server application session modules:	Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including: • The Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server • The VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM) • The QoS Device Manager (QDM) application, which uses the QDM Server • The IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS) **Note** 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.
HTTP server current connections:	Currently active HTTP connections.
HTTP server statistics:	How many connections have been accepted.
HTTP server history:	Details about the last 20 connections, including the time the connection was closed (endtime). Endtime is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format: *hh*:*mm*:*ss month*/*day*

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
debug ip http server all	Enables debugging output for all HTTP processes on the system.
ip http secure-server	Enables the HTTPS server.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.
show ip http server secure status	Displays the status of the HTTPS server.

Feature Information for the HTTP 1.1 Web Server and Client

Table 7 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 7 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 7 Feature Information for the HTTP 1.1 Web Server and Client

Feature Name	Releases	Feature Information
HTTP 1.1 Web Server and Client	12.2(31)SB2	The HTTP 1.1 Web Server and Client feature provides a consistent interface for users and applications by implementing support for HTTP 1.1 in Cisco IOS software-based devices. The integrated HTTP server API supports server application interfaces and provides a complete solution for HTTP services to and from Cisco devices. **Note** HTTPS is not supported in this release.