



Transferring Files Using HTTP or HTTPS

First Published: May 5, 2005

Last Updated: May 14, 2009

Cisco IOS Release 12.4 provides the ability to transfer files between your Cisco IOS software-based device and a remote HTTP server using the HTTP or HTTP Secure (HTTPS) protocol. HTTP and HTTPS can now be specified as the targets and source locations in Cisco IOS command-line interface (CLI) commands that use file system prefixes such as the **copy** command.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Transferring Files Using HTTP or HTTPS” section on page 14](#).

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

- [Prerequisites for Transferring Files Using HTTP or HTTPSs, page 2](#)
- [Restrictions for Transferring Files Using HTTP or HTTPSs, page 2](#)
- [Information About File Transfers Using HTTP or HTTPSs, page 2](#)
- [How to Transfer Files Using HTTP or HTTPSs, page 2](#)
- [Configuration Examples for the File Transfer Using HTTP or HTTPSs, page 10](#)
- [Additional References, page 11](#)
- [Feature Information for Transferring Files Using HTTP or HTTPSs, page 14](#)



Americas Headquarters:

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

Prerequisites for Transferring Files Using HTTP or HTTPS

To copy files to or from a remote HTTP server, your system must support the HTTP client feature, which is integrated in most Cisco IOS software images. The HTTP client is enabled by default. To determine if the HTTP client is supported on your system, issue the **show ip http client all** command. If you are able to execute the command, the HTTP client is supported.

Commands exist for the optional configuration of the embedded HTTP client and for the HTTPS client, but the default configuration is sufficient for using the File Transfer Using HTTP or HTTPS feature. For information on configuring optional HTTP or HTTPS client characteristics, see the [“Related Documents” section on page 12](#).

Restrictions for Transferring Files Using HTTP or HTTPS

Existing limitations to the **copy** command, such as no network-to-network copies, are in effect for the File Transfer Using HTTP or HTTPS feature.

**Note**

The **copy** command in Cisco IOS Release 12.4T does not work in conjunction with older versions of the Apache server software. The Apache server software must be upgraded to version 2.0.49 or later in order to use the copy command.

Information About File Transfers Using HTTP or HTTPS

To transfer files using HTTP or HTTPS, you should understand the following concept:

The File Transfer Using HTTP or HTTPS feature provides the capability to copy files, such as Cisco IOS image files, core files, configuration files, log files, scripts, and so on, to and from a remote server and your local routing device using the Cisco IOS **copy** command and command-line interface. The HTTP copy operation works in the same way as copying from other remote file systems, such as FTP or TFTP.

The HTTP copy operation can use the embedded HTTPS client for HTTP Secure transfers, providing secure and authenticated file transfers within the context of a public key infrastructure (PKI).

How to Transfer Files Using HTTP or HTTPS

This section contains the following procedures:

- [Configuring HTTP Connection Characteristics for File Transfers, page 3](#) (as required)
- [Downloading a File from a Remote Server Using HTTP or HTTPS, page 5](#) (required)
- [Uploading a File to a Remote Server Using HTTP or HTTPS, page 7](#) (required)
- [Maintaining and Monitoring File Transfers Using HTTP, page 9](#) (optional)

**Note**

To use the File Transfer Using HTTP feature, you may need to specify a username and password for the HTTP connections for those servers that require a username and password to connect. Commands are also available to specify custom connection characteristics, although default settings can be used. The feature also offers commands to monitor and maintain connections and files.

Configuring HTTP Connection Characteristics for File Transfers

Default values are provided for HTTP File transfers. The following task is used to customize the connection characteristics for your network to specify a username and password, connection preferences, a remote proxy server, and the source interface to be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http client connection {forceclose | idle timeout *seconds* | timeout *seconds*}**
4. **ip http client username *username***
5. **ip http client password *password***
6. **ip http client proxy-server {*proxy-name* | *ip-address*} [**proxy-port** *port-number*]**
7. **ip http client source-interface *interface-id***
8. **do copy running-config startup-config**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip http client connection {forceclose idle timeout seconds timeout seconds}</p> <p>Example: Router(config)# ip http client connection timeout 15</p>	<p>Configures characteristics for HTTP client connections to a remote HTTP server for all file transfers:</p> <ul style="list-style-type: none"> forceclose—Disables the default persistent connection. idle timeout seconds—Sets the period of time allowed for an idle connection, in a range from 1 to 60 seconds. Default timeout is 30 seconds. timeout seconds—Sets the maximum time the HTTP client waits for a connection, in a range from 1 to 60 seconds. Default is 10 seconds.
Step 4	<p>ip http client username username</p> <p>Example: Router(config)# ip http client username user1</p>	<p>Specifies the username to be used for HTTP client connections that require user authentication.</p> <p>Note You can also specify the username on the CLI when you issue the copy command, in which case the username entered overrides the username entered with this command. See the “Downloading a File from a Remote Server Using HTTP or HTTPS: Example” section on page 10 for an example.</p>
Step 5	<p>ip http client password password</p> <p>Example: Router(config)# ip http client password letmein</p>	<p>Specifies the password to be used for HTTP client connections that require user authentication.</p> <p>Note You can also specify the password on the CLI when you issue the copy command, in which case the password entered overrides the password entered with this command. See the “Downloading a File from a Remote Server Using HTTP or HTTPS: Example” section on page 10 for an example.</p>

	Command or Action	Purpose
Step 6	<pre>ip http client proxy-server {proxy-name ip-address} [proxy-port port-number]</pre> <p>Example: Router(config)# ip http client proxy-server edge2 proxy-port 29</p>	<p>Configures the HTTP client to connect to a remote proxy server for HTTP file system client connections.</p> <ul style="list-style-type: none"> The optional proxy-port <i>port-number</i> keyword and argument specify the proxy port number on the remote proxy server.
Step 7	<pre>ip http client source-interface interface-id</pre> <p>Example: Router(config)# ip http client source-interface Ethernet 0/1</p>	<p>Specifies the interface for the source address in all HTTP client connections.</p>
Step 8	<pre>do copy running-config startup-config</pre> <p>Example: Router(config)# do copy running-config startup-config</p>	<p>(Optional) Saves the running configuration as the startup configuration file.</p> <ul style="list-style-type: none"> The do command allows you to execute privileged EXEC mode commands from global configuration mode.
Step 9	<pre>end</pre> <p>Example: Router(config)# end Router#</p>	<p>Ends your configuration session and returns the CLI to user EXEC mode.</p>

Downloading a File from a Remote Server Using HTTP or HTTPS

Perform this task to download a file from a remote HTTP server using HTTP or HTTPS. The **copy** command helps you to copy any file from a source to a destination.

SUMMARY STEPS

- enable**
- copy** [/erase] [/noverify] **http://remote-source-url local-destination-url**
or
copy https://remote-source-url local-destination-url

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>copy [/erase] [/noverify] http://remote-source-url <i>local-destination-url</i></p> <p>or</p> <p>copy https://remote-source-url <i>local-destination-url</i></p> <p>Example: Router# copy http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx flash:c7200-i-mx</p> <p>Example: Router# copy copy https://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx flash:c7200-i-mx</p>	<p>Copies a file from a remote web server to a local file system using HTTP or HTTPS.</p> <ul style="list-style-type: none"> /erase—Erases the local destination file system before copying. This option is provided on Class B file system platforms with limited memory to allow an easy way to clear local flash memory space. /noverify—If the file being copied is an image file, this keyword disables the automatic image verification that occurs after an image is copied. The <i>remote-source-url</i> argument is the location URL (or alias) from which to get the file to be copied, in standard Cisco IOS file system HTTP syntax as follows: http://[[username:password]@] {hostname host-ip}[/filepath]/filename <p>Note The optional <i>username</i> and <i>password</i> arguments can be used to log in to an HTTP server that requires user authentication, in place of configuring the ip http client username and ip http client password global configuration commands to specify these authentication strings.</p> <ul style="list-style-type: none"> The <i>local-destination-url</i> is the location URL (or alias) to put the copied file, in standard Cisco IOS file system syntax as follows: filesystem:[/filepath]/filename <p>Note For more information on URL syntax when you use the copy command, see the “Additional References” section on page 11.</p>

Troubleshooting Tips

If file transfers from a remote web server fail, verify the following:

- Your router has an active connection to the Internet.
- The correct path and filename have been specified.
- The remote server requires a username and password.
- The remote server has a nonstandard communications port configured. (The default port for HTTP is 80; the default port for HTTPS is 443.)

The CLI returns error messages to help you determine the cause of a failed copy request. Additional information on the copy process can be displayed with the **debug ip http client all** command.

Uploading a File to a Remote Server Using HTTP or HTTPS

Perform this task to upload a file to a remote HTTP server using HTTP or HTTPS.

SUMMARY STEPS

1. **enable**
2. **copy** [*/erase*] [*/noverify*] *local-source-url* **http://remote-destination-url**
or
copy *local-source-url* **https://remote-destination-url**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>copy [/erase] [/noverify] local-source-url http://remote-destination-url</pre> <p>or</p> <pre>copy local-source-url https://remote-destination-url</pre> <p>Example: Router# http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx_backup</p> <p>Example: Router# copy flash:c7200-i-mx http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx_backup</p>	<p>Copies a file from a local file system to a remote web server using HTTP or HTTPS.</p> <ul style="list-style-type: none"> /erase—Erases the local destination file system before copying. This option is provided on Class B file system platforms with limited memory to allow an easy way to clear local flash memory space. /noverify—If the file being copied is an image file, this keyword disables the automatic image verification that occurs after an image is copied. The <i>local-source-url</i> argument is the location URL (or alias) from which to get the file to be copied, in standard Cisco IOS file system syntax as follows: http://[[username:password]@] {hostname host-ip}[/filepath]/filename <p>Note The optional <i>username</i> and <i>password</i> arguments can be used to log in to an HTTP server that requires user authentication, in place of configuring the ip http client username and ip http client password global configuration commands to specify these authentication strings.</p> <ul style="list-style-type: none"> The <i>remote-destination-url</i> is the URL (or alias) to put the copied file, in standard Cisco IOS file system syntax, as follows: <i>filesystem:[/filepath]/filename</i> <p>Note For more information on URL syntax when you use the copy command, see the “Additional References” section on page 11.</p>

Troubleshooting Tips

If file transfers from a remote web server fail, verify the following:

- Your router has an active connection to the Internet.
- The correct path and filename have been specified.
- The remote server requires a username and password.
- The remote server has a nonstandard communications port configured. (The default port for HTTP is 80; the default port for HTTPS is 443.)

The CLI returns error messages to help you determine the cause of a failed copy request. Additional information on the copy process can be displayed with the **debug ip http client all** command.

Maintaining and Monitoring File Transfers Using HTTP

Perform this task to maintain and monitor HTTP connections. Steps 2 through 4 can be performed in any order.

SUMMARY STEPS

1. `enable`
2. `show ip http client connection`
3. `show ip http client history`
4. `show ip http client session-module`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip http client connection Example: Router# show ip http client connection	Displays details about active HTTP client connections.
Step 3	show ip http client history Example: Router# show ip http client history	Displays the last 20 URLs accessed by the HTTP client.
Step 4	show ip http client session-module Example: Router# show ip http client session-module	Displays details about sessions (applications) that have registered with the HTTP client.

Related Documents

Related Topic	Document Title
Secure HTTP communications	<i>HTTPS —HTTP Server and Client with SSL 3.0</i>
Cisco IOS embedded web server	<i>HTTP 1.1 Web Server and Client</i>
Cisco IOS embedded web client	<i>HTTP 1.1 Client</i>
Network Management Commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Network Management Command Reference</i>
Configuration Fundamentals Commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Configuration Fundamentals Command Reference</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
None	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	<i>Hypertext Transfer Protocol -- HTTP/1.1</i> , R. Fielding, et al.
RFC 2617	<i>HTTP Authentication: Basic and Digest Access Authentication</i> , J. Franks, et al.

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Transferring Files Using HTTP or HTTPS

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

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/fn>. An account on Cisco.com is not required.


Note

Table 1 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 1 Feature Information for Transferring Files Using HTTP or HTTPS

Feature Name	Releases	Feature Information
File Download Using HTTP	12.3(2)T	<p>The File Download Using HTTP feature allows you to copy files from an HTTP server to a Cisco IOS software-based platform.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Downloading a File from a Remote Server Using HTTP or HTTPS, page 5
File Upload Using HTTP	12.3(7)T	<p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • “Uploading a File to a Remote Server Using HTTP or HTTPS” section on page 7
File Transfer Using HTTP	12.3(7)T	<p>The File Transfer Using HTTP feature provides the capability to copy files, such as Cisco IOS image files, core files, configuration files, log files, and scripts to and from a remote server and your local routing device using the Cisco IOS copy command and command-line interface. The HTTP copy operation works in the same way as copying from other remote file systems, such as FTP or TFTP.</p> <p>This feature provides support for copying files from a Cisco IOS software-based platform to an HTTP server, using either HTTP or HTTPS.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • “Information About File Transfers Using HTTP or HTTPS” section on page 2 • “How to Transfer Files Using HTTP or HTTPS” section on page 2

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.

