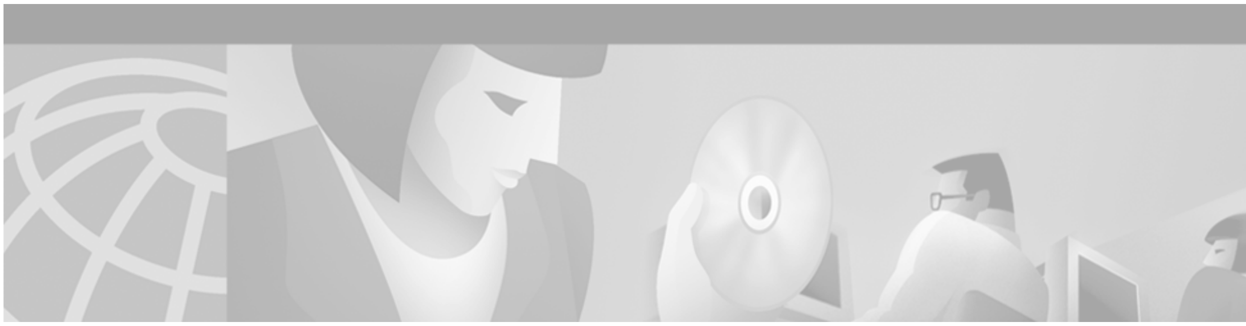


# Release Notes for Cisco Cache Software, Release 2.3.0

**November 3, 2000**

> **Note** The most current Cisco documentation for released products is available on Cisco Connection Online (CCO) at http://www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were printed.

## Contents

These release notes describe the following topics:

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

# Introduction

These release notes describe new commands included in Cisco Cache Software, Release 2.3.0 for the Cisco Content Engines and Cisco Cache Engines. To simplify terminology, both the Cache Engine and the Content Engine are referred to as the "CE." Refer to the *Cisco Cache Software Configuration Guide* for the following information:

- Instructions for configuring and maintaining the Cisco Cache Software
- Descriptions of Web Cache Communication Protocol (WCCP) Version 1 and Version 2

Refer to the *Cisco Cache Software Command Reference, Release 2.3.0* for global configuration, EXEC, show, and interface command descriptions. See the *Cisco Content Engine 500 Series Hardware Installation Guide* for information on the Cisco Content Engines.

**Note** WCCP is variously known as the Web Cache Control Protocol, and the Web Cache Coordination Protocol.

# Determining the Operating Software Version

**Note** We recommend that you install the most recent software release available for your model of the CE.

To determine the version of the software currently running on the Cisco CE, log on to the CE and enter the **show version** EXEC command.

## Downloading Cache Software

CE Cache software can be downloaded from the Cisco Systems Software Center at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cache-engine

## Upgrading to a New Software Release

As of the date of this release note, two types of CE Cache software files are available on CCO to download: files with the .pax suffix and files with the .bin suffix. The .pax file contains the full-image software with the graphical user interface (GUI) and is the file routinely installed. The .bin file software is for recovery situations that require booting from the network, or restoring Flash memory. Refer to the section "Recovering the System Software" in the *Cisco Cache Software Configuration Guide* for instructions on loading your system image with the .bin file.

**Step 1** Use an FTP client to transfer the .pax file to the */local* directory of your CE.

**Step 2** Log on to the CE, and at the priveleged level EXEC command prompt enter:

```
install filename.pax
```

where *filename* is the name of the .pax file.

**Step 3** Follow the command-line interface instructions as prompted. At the following prompt, enter **y**:

```
Copy new image to flash memory?[yes]:
```

**Step 4** After the CE has rebooted, use the **show version command** to display the current software version.

# New and Changed Information

## New Hardware Features in Cache Software Release 2.3.0

Release 2.3.0 of the Cisco Cache software adds support for the Content Engine 507, 560 and 590.

## New Software Features in Cache Software Release 2.3.0

- FTP Caching, page 3
- Proxy Failover, page 12
- TACACS+ Support, page 21

Release 2.3.0 operates all models of the Cisco 500 Series Cache Engines as well as the Cisco Content Engine 590, 507, and 560. To simplify terminology, both the Cache Engine and the Content Engine are referred to as the "CE" in this document.

## FTP Caching

The CE can fulfill File Transfer Protocol (FTP) requests, and cache FTP content for web clients that are configured to use the CE as a proxy server. The **ftp** global configuration command was added to the command line interface (CLI).

### ftp Command

Use the **ftp** global configuration command to configure FTP caching services on the CE. Use the **no** form of the command to selectively disable options.

**ftp** {**age-multiplier directory-listing** *dl_time* **file** *fo_time* | **max-ttl** {**days directory-listing** *dlmax_days* **file** *fmax_days* | **hours directory-listing** *dlmax_hours* **file** *fmax_hours* | **minutes directory-listing** *dlmax_ min* **file** *fmax_min* | **seconds directory-listing** *dlmax_ sec* **file** *fmax_sec*} | **min-ttl** *min_minutes* | **object max-size** *size* | **proxy** {**anonymous-pswd** *passwd* | **incoming** *port* | **outgoing host** {*hostname* | *ipaddress*} *port*} | **reval-each-request** {**all** | **directory-listing** | **none**} | **serve-ims directory-listing** *age_percent* **file** *age_percent*}

**no ftp** {**age-multiplier directory-listing** *dl_time* **file** *fo_time* | **max-ttl** {**days directory-listing** *dlmax_days* **file** *fmax_days* | **hours directory-listing** *dlmax_hours* **file** *fmax_hours* | **minutes directory-listing** *dlmax_ min* **file** *fmax_min* | **seconds directory-listing** *dlmax_ sec* **file** *fmax_sec*} | **min-ttl** *min_minutes* | **object max-size** *size* | **proxy** {**anonymous-pswd** *passwd* | **incoming** *port* | **outgoing host** {*hostname* | *ipaddress*} *port*} | **reval-each-request** {**all** | **directory-listing** | **none**} | **serve-ims directory-listing** *age_percent* **file** *age_percent*}

## Syntax Description

| | |
|---|---|
| **age-multiplier** | FTP caching heuristic modifiers. |
| **directory-listing** | Heuristic modifier for directory listing objects. |
| *dl_time* | Expiration time of directory listing objects as a percentage of their age (0–100). The default is 30. |
| **file** | Heuristic modifier for file objects. |
| *fo_time* | Expiration time of file objects as a percentage of their age (0–100). The default is 60. |
| **max-ttl** | Sets maximum Time To Live for objects in the cache. |
| **days** | Sets maximum Time To Live units in days. |
| **directory-listing** | Sets maximum Time To Live for directory listing objects in days. |
| *dlmax_days* | Specifies maximum Time To Live in days for directory listing objects (1–1825). The default is 7 days. |
| **file** | Sets maximum Time To Live for file objects in days. |
| *fmax_days* | Specifies the maximum Time To Live in days (1–1825). The default is 3 days. |
| **hours** | Sets maximum Time To Live units in hours. |
| **directory-listing** | Sets maximum Time To Live for directory listing objects in hours. |
| *dlmax_hours* | Specifies maximum Time To Live for directory listing objects in hours (1–43800). The default is 72 hours. |
| **file** | Sets maximum Time To Live for file objects in hours. |
| *fmax_hours* | Specifies the maximum Time To Live for file objects in hours (1–43800). The default is 168 hours. |
| **minutes** | Sets maximum Time To Live units in minutes. |
| **directory-listing** | Sets maximum Time To Live for directory listing objects in minutes. |
| *dlmax_ min* | Specifies the maximum Time To Live for directory listing objects in minutes (1–2628000). The default is 4320 minutes. |
| **file** | Sets maximum Time To Live for file objects in minutes. |
| *fmax_min* | Specifies the maximum Time To Live for file objects in minutes (1–2628000). The default is 10080 minutes. |
| **seconds** | Sets maximum Time To Live units in seconds. |
| **directory-listing** | Sets maximum Time To Live for directory listing objects in seconds. |
| *dlmax_ sec* | Specifies the maximum Time To Live for directory listing objects in seconds (1–157680000). The default is 259200 seconds. |
| **file** | Sets maximum Time To Live for file objects in seconds. |
| *fmax_sec* | Specifies the maximum Time To Live for file objects in seconds (1–157680000). The default is 604800 seconds. |
| **min-ttl** | Sets minimum Time To Live for FTP objects in cache. |

| | |
|---|---|
| *min_minutes* | Specifies the minimum Time To Live in minutes for FTP objects in cache (0–86400). |
| **object** | Sets configuration of FTP objects. |
| **max-size** | Sets maximum size of a cachable object. |
| *size* | Specifies the maximum size of a cachable object in KB (1–1048576). |
| **proxy** | Sets proxy configuration parameters. |
| **anonymous-pswd** | Sets anonymous password string (for example, wwwuser@cisco.com). |
| *passwd* | Specifies the anonymous password. The default is anonymous@hostname. |
| **incoming** | Sets the incoming port for proxy-mode requests. |
| *port* | Specifies up to eight ports to listen for requests (1–65535). |
| **outgoing** | Sets parameters to direct outgoing FTP requests to another proxy server. |
| **host** | Sets outgoing FTP proxy host parameters. |
| *hostname* | Specifies the hostname of the outgoing FTP proxy. |
| *ipaddress* | Specifies the IP address of the outgoing FTP proxy. |
| *port* | Specifies the port of the outgoing FTP proxy (1–65535). |
| **reval-each-request** | Sets scope of revalidation for every request. |
| **all** | Revalidates all objects on every request. |
| **directory-listing** | Revalidates directory listing objects on every request. |
| **none** | Does not revalidate for each request. |
| **serve-ims** | Sets the handling of “if-modified-since” requests. |
| **directory-listing** | Modifies handling of “if-modified-since” requests for directory listing objects. |
| *age_percent* | Specifies the percentage of age to serve the object without revalidation (0–100). The default is 50. |
| **file** | Modifies handling of if-modified-since requests for file objects. |
| *age_percent* | Specifies percentage of age to serve the object without revalidation (0–100). The default is 80. |

## Defaults

- *dl_time* is 30 percent.
- *fo_time* is 60 percent.
- *dlmax_days* is 7 days.
- *fmax_days* is 3 days.
- *dlmax_hours* is 72 hours.
- *fmax_hours* is 168 hours.
- *dlmax_min* is 4320 minutes.
- *fmax_min* is 10080 minutes.
- *dlmax_sec* is 259200 seconds.
- *fmax_sec* is 604800 seconds.
- *min_minutes* is 86400 minutes.
- **directory-listing** *age_percent* is 50 percent.

- **file** *age_percent* is 80 percent.

### Command Modes

Global configuration

### Usage Guidelines

The CE can fulfill ftp:// style FTP requests over HTTP transport in proxy mode.

When the CE receives an FTP request from the Web client, it first looks in its cache. If the object is not in its cache, it fetches the object from an upstream FTP proxy server (if one is configured), or directly from the origin FTP server.

The CE caches both the FTP file objects and directory listings. The content (directory listings and files) is stored in CFS.

The FTP proxy supports passive and active mode for fetching files and directories. Passive mode is the default. The CE automatically changes to active mode if passive mode is not supported by the FTP server.

The FTP proxy supports anonymous as well as authenticated FTP requests. Only base64 encoding is supported for authentication. The FTP proxy accepts all FTP URL schemes defined in RFC 1738. In the case of a URL in the form ftp://user@site/dir/file, the proxy sends back an authentication failure reply and the browser supplies a popup window for the user to enter login information.

The FTP proxy supports commonly used MIME types, attaches the corresponding header to the client, chooses the appropriate transfer type (binary or ASCII), and enables the browser to open the FTP file with the configured application. For unknown file types, the proxy uses binary transfer as default and instructs the browser to save the download file instead of opening it. The FTP proxy returns a formatted directory listing to the client if the FTP server replies with a known format directory listing. The formatted directory listing has full information about the file or directory and provides the ability for users to choose the download transfer type.

The CE caches FTP traffic only when the client uses the CE as a proxy server for FTP requests. All FTP traffic that was sent directly from the Web client to an FTP server, if transparently intercepted by the CE, is treated as non-HTTP traffic.

The FTP proxy supports up to eight incoming ports. It can share the ports with transparent-mode services and also with the other proxy-mode protocols supported by the CE, such as HTTP and HTTPS. In proxy-mode, the CE accepts and services the FTP requests only on the ports configured for FTP proxy. All the FTP requests on other proxy-mode ports are rejected in accordance with the error-handling settings on the CE.

The CE can apply the rules template to FTP requests based on server name, domain name, server IP address and port, client IP address, and URL.

The CE logs FTP transactions in the transaction log, in accordance with the Squid syntax. When URL tracking is enabled, the CE logs FTP transaction information to the syslog. The syslog entries are prefixed with <ftp>.

### Examples

This example configures an incoming FTP proxy on ports 8080, 8081, and 9090. Up to eight incoming proxy ports can be configured on the same command line.

```
CE(config)# ftp proxy incoming 8080 8081 9090
```

This example removes one FTP proxy port from the list entered in the previous example. Ports 8080 and 9090 remain FTP proxy ports.

```
CE(config)# no ftp proxy incoming 8081
```

This example disables all the FTP proxy ports.

```
CE(config)# no ftp proxy incoming
```

This example configures an upstream FTP proxy with the IP address 172.76.76.76 on port 8888.

```
CE(config)# ftp proxy outgoing host 172.76.76.76 8888
```

This example specifies an anonymous password string for the CE to use when contacting FTP servers. The default password string is anonymous@hostname.

```
CE(config)# ftp proxy anonymous-pswd newstring@hostname
```

This example configures the maximum size in kilobytes of an FTP object that the CE will cache. By default, the maximum size of a cachable object is not limited.

```
CE(config)# ftp object max-size 15000
```

This example forces the CE to revalidate all objects for every FTP request.

```
CE(config)# ftp reval-each-request all
```

This example configures a maximum Time To Live of 3 days in cache for directory listing objects and file objects.

```
CE(config)# ftp max-ttl days directory-listing 3 file 3
```

### Related Commands

**rule use-proxy**

**show ftp**

**show statitics ftp**

## show ftp Command

To display the configuration of the File Transfer Protocol (FTP) on the CE, use the **show ftp** command.

**show ftp**

### Syntax Description

The **show ftp** command has no keywords or options.

### Defaults

No default behavior or values

### Command Modes

EXEC

### Examples

```
Console# show ftp

FTP heuristic age-multipliers: directory-listing 30% file 60%
Maximum time to live in days : directory-listing 3 file 7
Minimum time to live in minutes: 60
No objects are revalidated on every request.
Serve-IMS without revalidation if...
Directory listing object is less than 50% of max age
File object is less than 80% of max age
Incoming Proxy-Mode:
Servicing Proxy mode FTP connections on ports: 22 23 88 66 48 488 449 90
Outgoing Proxy-Mode:
Not using outgoing proxy mode.
Maximum size of a cachable object is unlimited.
Console#
```

### Related Commands

**ftp**

**show statistics ftp**

## show statistics ftp Command

To display FTP related statistic, use the **show statistics ftp** option.

**show statistics ftp**

### Syntax Description

The **show statistics ftp** command has no keywords or options.

### Defaults

No default behavior or values

### Command Modes

EXEC

## Examples

```
CE# show statistics ftp
FTP Statistics
--------------
FTP requests Received = 9

FTP Hits
                                 Requests Percentage
 Number of hits =                       2       22.2 %
          Bytes =                   13542       22.0 %

FTP Misses
                                   Requests Percentage
 Number of misses =                       7       77.8 %
            Bytes =                   47946       78.0 %

 Requests sent to Outgoing Proxy    = 7
 Requests sent to origin ftp server = 0

FTP error count = 0
```

To clear the FTP caching statistics statistics:

```
CE# clear statistics ftp
```

## Related Commands

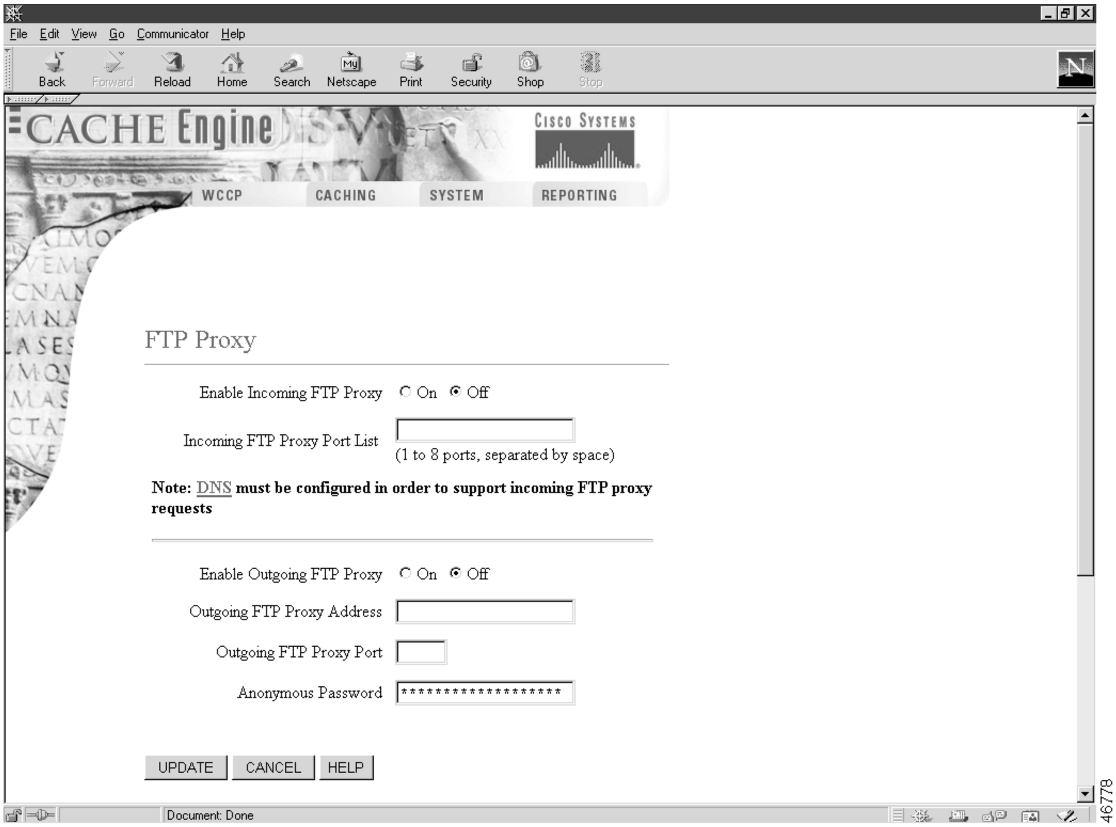
**ftp**

**show ftp**

## FTP Proxy Page

The FTP Proxy page has been added to the Caching menu, as shown in Figure 1. See the FTP Proxy online help for further information.

*Figure 1 Management GUI— FTP Proxy Page*



FTP Proxy

Enable Incoming FTP Proxy ○ On ● Off

Incoming FTP Proxy Port List (1 to 8 ports, separated by space)

**Note: DNS must be configured in order to support incoming FTP proxy requests**

Enable Outgoing FTP Proxy ○ On ● Off

Outgoing FTP Proxy Address

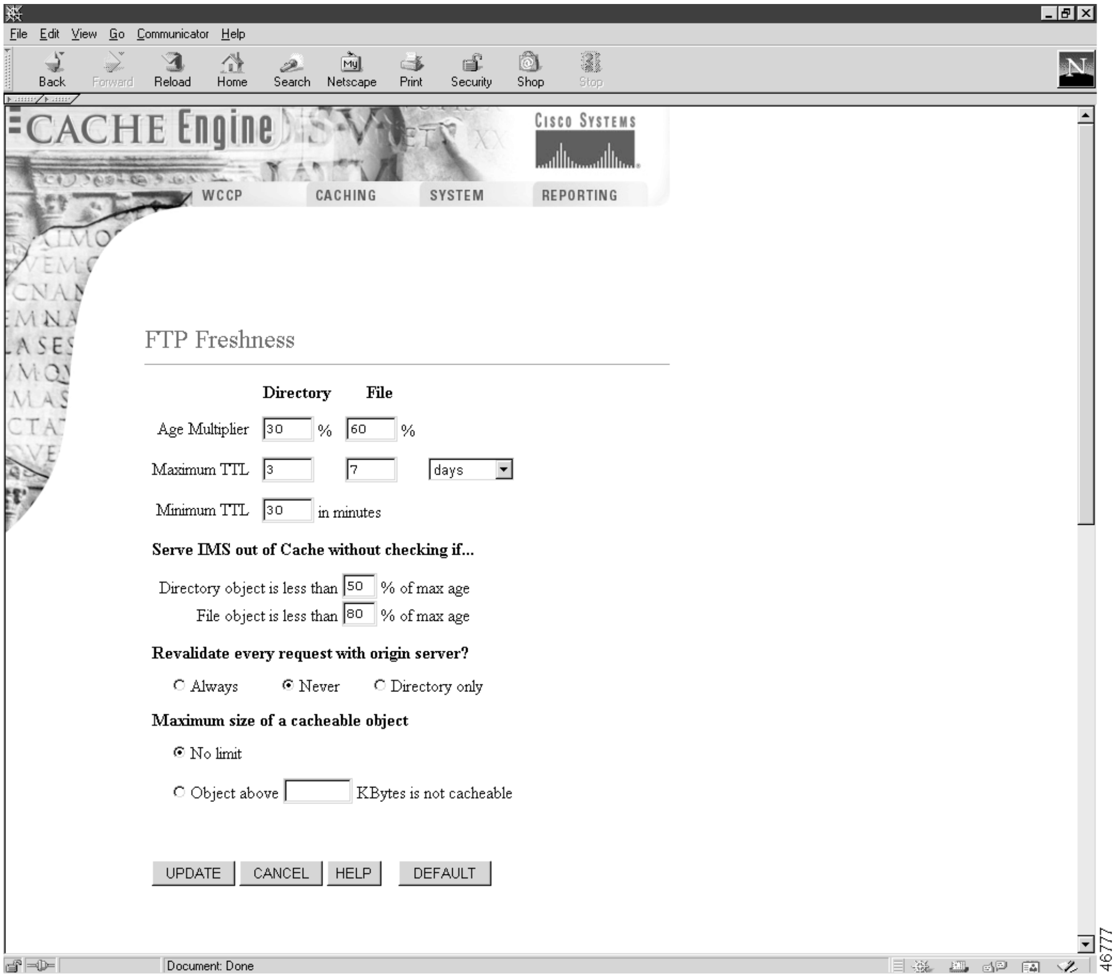
Outgoing FTP Proxy Port

Anonymous Password ********************

## FTP Freshness Page

The FTP Freshness page has been added to the Caching menu, as shown in Figure 3. See the FTP Freshness online help for further information.

*Figure 2 Management GUI— FTP Freshness Page*



FTP Freshness

| | Directory | File | |
|---|---|---|---|
| Age Multiplier | 30 % | 60 % | |
| Maximum TTL | 3 | 7 | days |
| Minimum TTL | 30 in minutes | | |

**Serve IMS out of Cache without checking if...**

Directory object is less than 50 % of max age
File object is less than 80 % of max age

**Revalidate every request with origin server?**

○ Always ● Never ○ Directory only

**Maximum size of a cacheable object**

● No limit

○ Object above KBytes is not cacheable

# Proxy Failover

The proxy failover feature reduces the incidence of server failure errors returned to the client. An administrator can configure a logical failover chain of outgoing HTTP proxy servers. One of the servers is designated as primary and receives the outgoing proxy traffic. If the primary server fails, the next server in the logical chain of proxy servers assumes the load. If that server fails, the next one takes over and so on. Use the **http proxy outgoing** global configuration command to configure up to eight failover outgoing proxies. The complete **http** syntax and usage guidelines are included to provide context.

## http Command

To configure HTTP-related parameters, use the **http** global configuration command. To disable HTTP related-parameters, use the **no** form of this command.

**http** {**age-multiplier** {**text** *texttime* **binary** *bintime*} | **append** {**ldap-proxy-auth-header** {*hostname* | *ipaddress*}| **via-header** | **x-forwarded-for-header**} | **authenticate-strip-ntlm** | **cache-authenticated** | **cache-cookies** | **cache-miss revalidate** | **cache-on-abort** {**enable** | **max** *maxthresh* | **min** *minthresh* | **percent** *percenthresh*} | **cluster max-delay** *delayseconds* **misses** *totalmisses* | **l4-switch enable | max-ttl** {**days text** *textdays* **binary** *bindays* | **hours text** *texthours* **binary** *binhours* | **minutes text** *textminutes* **binary** *binminutes* | **seconds text** *textseconds* **binary** *binseconds*} | **min-ttl** *minutes* | **object** {**max-size** *maxsize* | **url-validation enable**} | **persistent-connections** {**enable** | **max-idle** *connections* | **timeout** *secs* [**max-idle** *connections*]} | **proxy** {**incoming** *port* | **outgoing** {**host** {*hostname* | *ipaddress*} *port* [**primary**]} | **monitor** *seconds* | **origin-server**} | **reval-each-request** {**all** | **none** | **text**} | **serve-ims text** *textpercentage* **binary** *binpercentage*}

**no http** {**age-multiplier** {**text** *texttime* **binary** *bintime*} | **append** {**ldap-proxy-auth-header** {*hostname* | *ipaddress*}| **via-header** | **x-forwarded-for-header**} | **authenticate-strip-ntlm** | **cache-authenticated** | **cache-cookies** | **cache-miss revalidate** | **cache-on-abort** {**enable** | **max** *maxthresh* | **min** *minthresh* | **percent** *percenthresh*} | **cluster max-delay** *delayseconds* **misses** *totalmisses* | **l4-switch enable | max-ttl** {**days text** *textdays* **binary** *bindays* | **hours text** *texthours* **binary** *binhours* | **minutes text** *textminutes* **binary** *binminutes* | **seconds text** *textseconds* **binary** *binseconds*} | **min-ttl** *minutes* | **object** {**max-size** *maxsize* | **url-validation enable**} | **persistent-connections** {**enable** | **max-idle** *connections* | **timeout** *secs* [**max-idle** *connections*]} | **proxy** {**incoming** *port* | **outgoing** {**host** {*hostname* | *ipaddress*} *port* [**primary**]} | **monitor** *seconds* | **origin-server**} | **reval-each-request** {**all** | **none** | **text**} | **serve-ims text** *textpercentage* **binary** *binpercentage*}

### Syntax Description

| | |
|---|---|
| **age-multiplier** | HTTP/1.0 caching heuristic modifiers. |
| **text** | Heuristic modifier for text object. |
| *texttime* | Expiration time of text objects as a percentage of their age (0–100). |
| **binary** | Heuristic modifier for binary object. |
| *bintime* | Expiration time of binary objects as a percentage of their age (0–100). |
| **append** | Configures HTTP headers to be included by CE. |
| **ldap-proxy-auth-header** | Forwards “Proxy Authorization” headers in outbound requests. |
| *hostname* | Host name of upstream proxy or server that will perform LDAP authentication. |

| | |
|---|---|
| *ipaddress* | IP address of upstream proxy or server that will perform LDAP authentication. |
| **via-header** | Includes “Via” header in responses and replies. |
| **x-forwarded-for-header** | Notifies Web server of client’s IP address through “X-Forwarded-For” header. |
| **authenticate-strip-ntlm** | Strips NT LAN Manager (NTLM) authentication headers. |
| **cache-authenticated** | Caches and revalidates authenticated Web objects. |
| **cache-cookies** | Caches Web objects with associated cookies. |
| **cache-miss** | Configuration for the handling of “no-cache” requests. |
| **retrieve** | Retrieves the object from the point of origin. |
| **revalidate** | Revalidates the object with the origin before serving. |
| **cache-on-abort** | Sets cache-on-abort configuration options. |
| **enable** | Enables cache-on-abort feature. |
| **max** | Sets maximum threshold. |
| *maxthresh* | Value in kilobytes of maximum threshold (1–99999). Default is 256. |
| **min** | Sets minimum threshold. |
| *minthresh* | Value in kilobytes of minimum threshold (1–99999). Default is 32. |
| **percent** | Sets percent threshold. |
| *percenthresh* | Percentage value (1–99). Default is 80 percent. |
| **cluster** | Sets cache cluster configuration options. |
| **max-delay** | Maximum delay to wait for a response. |
| *delayseconds* | Maximum delay in seconds (0–10). |
| **misses** | Duration of healing mode (misses). |
| *totalmisses* | Total number of misses before healing is disabled (0–999). |
| **l4-switch enable** | Enables Layer 4 switch redirection. |
| **max-ttl** | Maximum Time To Live for objects in the cache. |
| **days** | Sets maximum Time To Live for units in days. |
| **hours** | Sets maximum Time To Live for units in hours. |
| **minutes** | Sets maximum Time To Live for units in minutes. |
| **seconds** | Sets maximum Time To Live for units in seconds. |
| **text** | Sets maximum Time To Live for text objects. |
| **binary** | Sets maximum Time To Live for binary objects. |
| *days* | Specifies maximum Time To Live for units in hours. |
| *hours* | Specifies maximum Time To Live for units in hours. |
| *minutes* | Specifies maximum Time To Live for units in minutes. |
| *seconds* | Specifies maximum Time To Live for units in seconds. |
| **min-ttl** | Sets minimum time for objects to live. |
| *minutes* | Specifies minimum time to live in minutes (0–86400). |
| **object** | Sets URL validation and maximum size of HTTP objects. |
| **max-size** | Sets the maximum size of a cachable object. |
| *maxsize* | Maximum size of a cachable object in kilobytes (1–1048576). |
| **url-validation enable** | Enables each HTTP validation request. |

| | |
|---|---|
| **persistent-connections** | Persistent connections configuration options. |
| **enable** | Enables persistent connections. |
| **max-idle** | Sets maximum number of idle persistent connections. |
| *connections* | Maximum number of idle persistent connections (1–4096). |
| **timeout** *secs* | Persistent connections timeout in seconds (1–86400). |
| **proxy** | Configuration parameters for proxy mode. |
| **incoming** | Configuration for incoming proxy-mode requests. |
| *port* | Port on which to listen for incoming HTTP proxy requests (1–65535). Default is port 8080. |
| **outgoing** | Configuration to direct outgoing request to another proxy server. |
| **host** | Use outgoing HTTP proxy. |
| *hostname* | Hostname of outgoing proxy. |
| *ipaddress* | IP address of outgoing proxy. |
| *port* | Port number of outgoing proxy (1–65535). |
| **primary** | (Optional.) Makes the proxy being configured the primary proxy server. |
| **monitor** | Interval at which to monitor the outgoing proxy servers. |
| *seconds* | Monitoring interval in seconds (10–300). |
| **origin-server** | Use origin server if all proxies are failed. |
| **reval-each-request** | Configuration of revalidation for every request. |
| **all** | Revalidates all objects on every request. |
| **none** | Does not revalidate for each request. |
| **text** | Revalidates text objects on every request. |
| **serve-ims** | Configuration for the handling of if-modified-since (IMS) requests for text objects. |
| **text** | Modifies handling of if-modified-since requests for text objects. |
| *textpercentage* | Percentage of age to serve the text object without revalidation (0–100). |
| **binary** | Modifies handling of if-modified-since requests for binary objects. |
| *binpercentage* | Percentage of age to serve the binary object without revalidation (0–100). |

## Defaults

See the corresponding syntax description for default values.

## Command Modes

Global configuration

## Usage Guidelines

### HTTP Proxy Failover Option

The **http proxy outgoing** option configures backup proxy servers for HTTP proxy failover support. One proxy server functions as the primary proxy server and all requests are redirected to it. If the primary proxy server fails to respond to the HTTP CONNECT, the server is noted as failed and the requests are redirected to the next outgoing proxy server until one of the proxies service the request.

To explicitly designate the primary proxy, use the **primary** keyword. If several proxies are configured with the **primary** keyword, the last one configured overrides the others. Failover to a proxy server occurs in the order the proxy servers were configured. In the event that all the configured proxy servers fail, the CE can optionally redirect requests to the origin server if the user enters the **http proxy outgoing origin-server** option. If the user has configured the **origin-server** option, the CE directs HTTP requests to the original server specified in the HTTP header. If the option is not enabled, the client receives the error. Response errors and read errors are returned to the client, since it is not possible to detect whether these errors are generated at the origin server or at the proxy. Up to eight outgoing proxy servers can be configured for a single CE.

The state of the proxy servers is maintained by active monitoring, which occurs in the background. The state of the proxy servers can be seen in the CLI and syslog NOTICE messages. This interval is configured with the **http proxy outgoing monitor** option. This outgoing monitor interval is the frequency with which a single proxy server is polled. Only one proxy server is polled per interval. If more than one proxy server is configured, the delay is in multiple intervals of the monitor value. If one of the proxy servers is unavailable, the polling mechanism waits for the connect timeout before polling the next server.

The configuration specified by the **rule** command has precedence over any other configured proxy server. If an administrator created a **use-proxy** rule, the HTTP request is directed only to the proxy specified by the rule. For example:

- **rule use-prox**y *ipaddr1 port_number* **domain** *cisco.com*
- **rule use-proxy** *ipaddr1* **failover**

Requests to the domain “cisco.com” failover to the backup proxies if ipaddr1 is unavailable. Any other rule that uses ipaddr1 fails over to the backup proxies when *ipaddr1* fails. Each request is checked to determine if the protocol supports failover (currently, only HTTP). If so, those requests failover to the list of outgoing proxies configured with the **http proxy outgoing host** option. In the event that all proxy servers fail, the failover of the **rule** command sends the request to the origin server if the **http proxy outgoing origin-server** option is entered.

Requests with destinations included in the **proxy-protocols outgoing-proxy exclude** list bypass the CE proxy as well as the failover proxies.

When an HTTP request intended for another proxy server is intercepted by the CE in transparent mode, the CE forwards the request to the intended proxy server if the **proxy-protocols transparent original-proxy** command was entered.

The proxy failover feature currently supports only HTTP, and not HTTPS or FTP.

### Other HTTP Configuration Options

**Note** Text objects refer to HTML pages. Binary objects refer to all other Web objects (for example, GIFs or JPEGs).

If a cached object’s HTTP header does not specify an expiration time, the **age-multiplier** and **max-ttl** options provide a means for the CE to age cached objects. The CE’s algorithm to calculate an object’s cache expiration date is as follows:

Expiration date = (Today’s date – Object’s last modified date) * Freshness factor

The freshness factor is computed from the text and binary percentage parameters of the **age-multiplier** command. Valid age-multiplier values are 0 to 100 percent of the object’s age. Default values are 30 percent for text and 60 percent for binary objects. After the expiration date, the object is considered stale and subsequent requests result in a fresh retrieval by the CE.

The **max-ttl** option sets the upper limit on estimated expiration dates. An explicit expiration date in the HTTP header takes precedence over the configurable TTL (Time To Live).

The **serve-ims** option responds to an if-modified-since request issued from a client browser by serving the object directly from the cache without revalidating with the origin server whether the object is less than the configured percentage of its maximum age.

The **cache-cookies** option enables the CE to cache binary served with HTTP set-cookies headers and no explicit expiration information.

The **cache-authenticated** option enables the CE to cache authenticated content. If this command is enabled, the CE will not serve authenticated objects without first revalidating the authentication header attached to the cached object.

The **reval-each-request** option enables the CE to revalidate all objects requested from the cache, text objects only, or none at all.

The **cache-miss revalidate** option revalidates a cache-miss request forced by the client (shift-reload). The **cache-miss retrieve** option forces a new object retrieval.

Use the **object max-size** option to specify the maximum size in kilobytes of a cachable object. The default is no maximum size for a cachable object. The **no** form of the command resets the default value.

The **cluster** option modifies the healing mode parameters. A cluster refers to a group of two or more CEs within a single WCCP Version 2 environment. Healing mode describes the addition of a CE to an existing network, and the resulting "healing" time it takes to fill the cache with content. To disable healing mode, you must set the number of misses to 0.

The **proxy mode** option enables the CE to operate in environments where WCCP is not enabled, or where client browsers have previously been configured to use a legacy proxy server. You must configure the proxy incoming port to accept proxy-style requests using the **proxy incoming port** option.

To configure the CE to direct all HTTP miss traffic to a parent cache (without using ICP or WCCP), use the **proxy outgoing hostname port** option, in which *hostname* is the system name or IP address of the outgoing proxy server, and *port* is the port number designated by the outgoing (upstream) server to accept proxy requests.

The **cache-on-abort** option provides user-defined thresholds to determine whether or not the CE will complete the download of an object when the client has aborted the request. When the download of an object aborts before it is completed, the object is not stored on the CE or counted in the hit-rate statistics. Client abort processing occurs when a client of the CE aborts the download of a cachable object before the download is complete. Typically, a client aborts a download by clicking the Stop icon on the browser, or by closing the browser during a download.

If the **cache-on-abort** option is enabled and all cache-on-abort thresholds are disabled, then the CE always aborts downloading an object to the cache. If the CE determines that there is another client currently requesting the same object, downloading is not aborted. The CE only applies those thresholds that have been enabled.

The **l4-switch enable** option enables the CE to transparently receive redirected HTTP traffic from Layer 4 switches with transparency features. See the switch documentation for specific configuration information.

Configure the **http ldap-proxy-auth-header** global configuration option when the CE and an upstream server or proxy is performing LDAP authentication.

To prevent disclosure of a user's proxy authentication credentials to another host, the CE removes the HTTP Proxy-Authorization header from the HTTP request when it forwards the request. With LDAP authentication it is important that upstream proxies share the authentication credentials carried in the header. To prevent the CE from stripping out the HTTP Proxy-Authorization header, enter the **http append ldap-proxy-auth-header** global configuration command. The CE will forward the Proxy-Authorization header with credentials to the specified host name or IP address.

The **persistent-connections enable** command enables persistent connections on the CE. To configure the number of seconds the CE should wait for a connection response before it times out, use the **timeout** option. To set the number of seconds that the CE should allow an idle persistent connection to remain open, use the **max-idle** option.

The **http object url-validation** option has a dependency with the **ip name-server** CLI command. When the **ip name-server** option is not configured (for example, during transparent proxy), **http object url-validation** is dynamically turned off. When the **ip name-server** option is configured, **http object url-validation** is turned on automatically if and only if it was enabled.

**Caution** URL validation is on by default. Cisco Systems strongly recommends that you keep URL validation enabled, because disabling URL validation might make the CE vulnerable to corruption from the HTTP objects in the cache.

Use the **exclude list** option in the **http proxy outgoing** global configuration command to specify domains for which the CE will not use an upstream proxy.

Only one domain can be specified per command line. To specify multiple domains for proxy exclusion, iteratively execute the command for each domain. In the following example, cisco.com and the address 10.9.8.7 are proxy-excluded.

```
Console(config)# http proxy outgoing exclude list cisco.com
Console(config)# http proxy outgoing exclude list 10.9.8.7
```

The maximum number of no-proxy domains is 64. The CE will not use an upstream proxy for any domain that ends with a listed domain name. For example, if you specify cisco.com, the configured outgoing proxy server will be bypassed each time the CE tries to retrieve a Web page from videos.cisco.com, or personals.cisco.com.

For IP addresses, enter the full IP address or use the asterisk "*" as a wildcard for IP address fields as follows:

172.16.1.*

172.16.*.*

172.*.*.*

The syntax 172.16.*.* indicates that all requests to the domain host of 172.16.xxx.xxx will be excluded. Wildcard syntax does not support "0" or "?".

The following forms of wildcard specification are not supported:

172.*.10.2

172.31.1*.8

## Examples

In this example, the host 10.1.1.1 on port 8088 is designated the primary proxy server, and host 10.1.1.2 is a backup proxy server.

```
CE(config)# http proxy outgoing host 10.1.1.1 8088 primary
CE(config)# http proxy outgoing host 10.1.1.2 220
```

In this example, the CE is configured to redirect requests directly to the origin server in the event that all of the proxy servers fail.

```
CE(config)# http proxy outgoing origin-server
```

In this example, the CE is configured to monitor the proxy servers every 120 seconds.

```
CE(config)# http proxy outgoing monitor 120
```

To disable any of the above, use the **no** version of the command.

### Proxy Failover Show Commands

```
Console# show http proxy
Incoming Proxy-Mode:
  Servicing Proxy mode HTTP connections on ports:   8080

Outgoing Proxy-Mode:
  Primary proxy server: 172.69.63.150   port 1 Failed
  Backup proxy servers: 172.69.236.151  port 8005
                        172.69.236.152  port 123
                        172.69.236.153  port 65535 Failed
                        172.69.236.154  port 10
    Proxy monitor interval:   60 seconds
  Use Origin Server upon Proxy Failure.
```

### Statistics

```
Console# show statistics http requests
                              Statistics - Requests
                                                Total             % of Requests
                             ---------------------------------------------------
     Total Received Requests:                      43                          -
              Forced Reloads:                       0                        0.0
                   Near Hits:                       0                        0.0
               Server Errors:                       0                        0.0
                 URL Blocked:                       0                        0.0
      Sent to Outgoing Proxy:                      32                       74.4
Failures from Outgoing Proxy:                       0                        0.0
Excluded from Outgoing Proxy:                      11                       25.6
             ICP Client Hits:                       0                        0.0
             ICP Server Hits:                       0                        0.0
           HTTP 0.9 Requests:                       0                        0.0
           HTTP 1.0 Requests:                      43                      100.0
           HTTP 1.1 Requests:                       0                        0.0
       HTTP Unknown Requests:                       0                        0.0
           Non HTTP Requests:                       0                        0.0
          Non HTTP Responses:                       0                        0.0
      Chunked HTTP Responses:                       0                        0.0
Flow-controlled HTTP streams:                       2                        4.7
        Http Miss Due To DNS:                       0                        0.0
     Http Deletes Due to DNS:                       0                        0.0
  Objects cached for min ttl:                       0                        0.0


Console# show statistics http proxy out
                    HTTP Outgoing Proxy Statistics
                    Attempts    Failures        Successes        Cleared
                   ----------------------------------------------------
       10.1.1.1:        0              1               0               0
 172.31.227.111:       32              0               0              40

 Requests when all proxies were failed: 0

Console(config)# http append ldap-proxy-auth-header ?
Hostname or A.B.C.D  IP address or hostname of proxy/server to receive proxy-auth headers
Console(config)# http append ldap-proxy-auth-header 172.16.1.1

Console(config)# http age-multiplier text 30 bin 60
Console(config)# http reval-each-request text
```

```
Console(config)# no http age-multiplier text 30 bin 60
```

```
Console(config)# no http reval-each-request text
```

- With the default configuration (all cache-on-abort thresholds disabled), configure client abort processing to always abort downloading an object to the cache:

  ```
  Console(config)# http cache-on-abort enable
  ```

- Configure the CE to always continue downloading an object to the cache (this is the default configuration):

  ```
  Console(config)# no http cache-on-abort
  ```

- Configure the CE to use the default minimum threshold when the cache-on-abort option has been enabled, and set the threshold to 16 kilobytes:

  ```
  Console(config)# http cache-on-abort min 16
  ```

- Configure the CE to not consider the minimum threshold:

  ```
  Console(config)# no http cache-on-abort min
  ```

  The **cache-on-abort max** and **percent** thresholds are configured like the minimum threshold shown in the examples.

### Related Commands

**ldap**

**proxy-protocols**

**rule no-proxy**

**rule use-proxy**

**show http**

**show http proxy**

**show ldap**

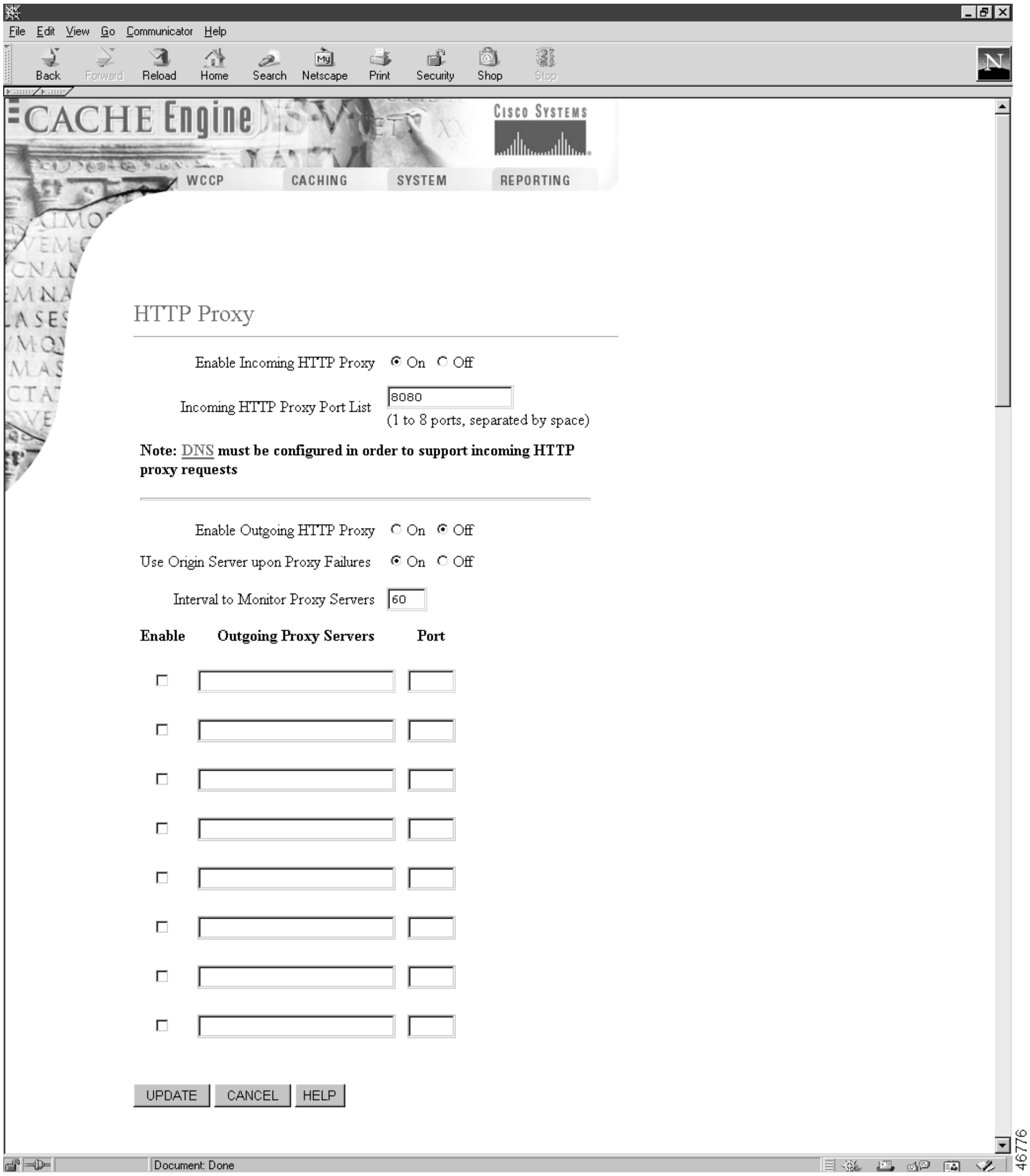
**show statistics http requests**

**show statistics http proxy outgoing**

## HTTP Proxy Page

The proxy failover feature is configured on the HTTP Proxy page in the Caching menu, as shown in Figure 3. See the HTTP Proxy online help for further information.

*Figure 3 Management GUI—HTTP Proxy Page*



HTTP Proxy

Enable Incoming HTTP Proxy ● On ○ Off

Incoming HTTP Proxy Port List 8080
(1 to 8 ports, separated by space)

**Note: DNS must be configured in order to support incoming HTTP proxy requests**

Enable Outgoing HTTP Proxy ○ On ● Off

Use Origin Server upon Proxy Failures ● On ○ Off

Interval to Monitor Proxy Servers 60

| Enable | Outgoing Proxy Servers | Port |
|---|---|---|
| ☐ | | |
| ☐ | | |
| ☐ | | |
| ☐ | | |
| ☐ | | |
| ☐ | | |
| ☐ | | |
| ☐ | | |

# TACACS+ Support

The Terminal Access Controller Access Control System (TACACS) validates users before they gain access to the router. TACACS is derived from the United States Department of Defense (RFC 1492) and is used by Cisco Systems as an additional control of non-privileged and privileged mode router access. Software Release 2.3.0 supports TACACS+ only and not TACACS or Extended TACACS. To configure TACACS+, use the **authentication** and **tacacs** commands.

## authentication Command

To configure Terminal Access Controller Access Control System Plus (TACACS+), authentication and authorization options, use the **authentication** global configuration command. Use the **no** form of the command to selectively disable options.

**authentication** {**configuration** {**local enable** | **tacacs enable** [**primary**]} | **login** {**local enable** | **tacacs enable** [**primary**]}}

**no authentication** {**configuration** {**local enable** | **tacacs enable** [**primary**]} | **login** {**local enable** | **tacacs enable** [**primary**]}}

### Syntax Description

| | |
|---|---|
| **configuration** | Sets authorization mode. |
| **local enable** | Enables local database for authorization. |
| **tacacs enable** | Enables TACACS+ database for authorization. |
| **primary** | (Optional.) Sets TACACS+ server authorization as a primary. |
| **login** | Sets authentication mode. |
| **local enable** | Enables local database for authentication. |
| **tacacs enable** | Enables TACACS+ database for authentication. |
| **primary** | (Optional.) Sets TACACS+ server authentication as a primary. |

### Defaults

Local authentication is enabled and TACACS+ authentication is disabled.

### Command Modes

Global configuration

### Usage Guidelines

Authentication or login is the action of identifying and validating a user. It verifies a username with the password. Authorization or configuration is the action of determining what a user is allowed to do.

Login and configuration privileges can be maintained in two databases: the local database, which resides on the CE, and the TACACS+ remote database, which resides on a remote server. The **user** global configuration commands or the Users GUI page provides a way to add, delete, or modify users' names, passwords, and access privileges in the local database. The TACACS+ remote database can also be used to maintain login and configuration privileges for CE administrative users. The **tacacs** command or the TACACS+ GUI page allows you to configure the network parameters required to access the remote database.

Login and configuration privileges can be obtained from both the local database or the TACACS+ remote database. If both databases are enabled, then both databases are queried; if the user data cannot be found in the first database queried, then the second database is tried. When the **primary** keyword is entered for TACACS+ login or configuration authentication (**authentication login tacacs enable primary**, **authentication configuration tacacs enable primary**), the TACACS+ database is queried first, and the local database is queried second. If TACACS+ is not designated as primary, and both local and TACACS+ are enabled, the local database is queried first. If both local and TACACS+ are disabled (**no authentication**), the CE verifies that both are disabled and if so, sets the CE to the default state.

By default, local authentication is enabled and TACACS+ authentication is disabled. When the TACACS+ authentication is disabled, the local authentication is automatically enabled.

## Examples

This example disables local configuration authentication.

```
CE(config)# no authentication configuration local
Local configuration authentication disabled.
```

**Note** If local authentication is disabled and TACACS+ is not configured properly, future logins may fail.

### TACACS+ Statistics

```
CE# show statistics authentication

Authentication Statistics
--------------------------------------
Number of Local Authentication: 0
Number of TACACS+ Authentication: 4
Total number of Authentication: 4

Number of Local Authorization: 0
Number of TACACS+ Authorization: 4
Total number of Authorization: 4

CE# show statistics tacacs
TACACS+ Statistics
-----------------
Number of access requests: 8
Number of access deny responses: 7
Number of access allow responses: 1
```

## Related Commands

**show authentication**

**show statistics authentication**

**show statistics tacacs**

**show tacacs**

**tacacs**

## show authentication Command

To display the current TACACS+ current authentication and authorization configuration, use the **show authentication** command.

**show authentication**

### Syntax Description

This command has no arguments or keywords.

### Defaults

No default behavior or values

### Command Modes

EXEC

### Examples

```
Console# show authentication
Login Authentication:         Console/Telnet Session
----------------------------- ----------------------
local                         enabled
tacacs                        enabled (primary)

Configuration Authentication: Console/Telnet Session
----------------------------- ----------------------
local                         enabled
tacacs                        enabled
```

## tacacs Command

To configure TACACS+ server-related parameters, use the **tacacs** global configuration command.

**tacacs** {**key** *keyword* | **retransmit** *retries* | **server** {*hostname* | *ipaddress*} [**primary**] | **timeout** *seconds*}

### Syntax Description

| | |
|---|---|
| **key** | Sets security word. |
| *keyword* | Specifies keyword. An empty string is the default. |
| **retransmit** | Sets number of times requests are retransmitted to a server. |
| *retries* | Specifies number of attempts allowed (1–10). The default is two retry attempts. |
| **server** | Sets a server address. |
| *hostname* | Specifies host name of TACACS+ server. |
| *ipaddress* | Specifies IP address of TACACS+ server. |
| **primary** | Sets server as primary. |
| **timeout** | Sets number of seconds to wait before a request to a server is timed out. |
| *seconds* | Specifies the timeout in seconds (1–255). The default is 5 seconds. |

### Defaults

An empty keyword string is the default. The default timeout time is 5 seconds. The default number of retry attempts is two.

### Command Modes

Global configuration

### Usage Guidelines

A TACACS+ server must be configured before you enable TACACS+ authentication on the CE. The CE can be configured to use the local password authentication if the TACACS+ password authentication fails. See the “authentication Command” section for more information.

Use the **tacacs key** command to specify the TACACS+ key, used to encrypt the packets transmitted to the server. This key must be the same as the one specified on the server daemon. The maximum number of characters in the key should not exceed 99 printable ASCII characters (except tabs). An empty key string is the default. All leading spaces are ignored; spaces within and at the end of the key string are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key.

One primary and two backup TACACS+ servers can be configured; authentication is attempted on the primary server first, then on the others in the order in which they were configured. The primary server is the first server configured unless another is explicitly specified as primary with the **tacacs server hostname primary** command.

The **tacacs timeout** is the number of seconds the CE waits before declaring a timeout on a request to a particular TACACS+ server. The range is from 1–255 seconds with 5 seconds as the default. The number of times the CE repeats a retry-timeout cycle before trying the next TACACS+ server is specified by the **tacacs retransmit** command. The default is two retry attempts.

Three unsuccessful login attempts are permitted. TACACS+ logins may appear to take more time than local logins depending on the number of TACACS+ servers and the configured timeout and retry values.

### Examples

This example configures the key used in encrypting packets.

```
CE(config)# tacacs key bronzemonkey789
```

This example configures the host named rasputin as the primary TACACS+ server.

```
CE(config)# tacacs server rasputin primary
```

This example sets the timeout interval for the TACACS+ server.

```
CE(config)# tacacs timeout 10
```

This example sets the number of times authentication requests are retried (retransmitted) after a timeout.

```
CE(config)# tacacs retransmit 5
```

### Related Commands

**authentication**

**show authentication**

**show statistics authentication**

**show statistics tacacs**

**show tacacs**

## show tacacs Command

To display the settings for the Terminal Access Controller Access Control System Plus (TACACS+) server, use the **show tacacs** EXEC command.

**show tacacs**

### Syntax Description

This command has no arguments or keywords.

### Defaults

No default behavior or values

### Command Modes

EXEC

### Examples

```
Console# show tacacs
Login Authentication for Console/Telnet Session: enabled (primary)
Configuration Authentication for Console/Telnet Session: enabled (primary)

TACACS Configuration:
---------------------
Key =
Timeout = 10 seconds
Retransmit = 2 times

Server Status
-------------------- ------
171.69.236.175 primary
171.69.227.254
```

You can also display login and configuration authentications using the **show authentication** command.

```
CE# show authentication
Login Authentication: Console/Telnet Session
----------------------------- -----------------------
local enabled
tacacs enabled (primary)

Configuration Authentication: Console/Telnet Session
----------------------------- -----------------------
local enabled
tacacs enabled (primary)
```

### Related Commands

**authentication**

**show authentication**

**show statistics tacacs**

**tacacs**

## show statistics tacacs Command

To display TACACS+ statistics, use the **show statistics tacacs** EXEC command.

**show statistics tacacs**

### Syntax Description

This command has no arguments or keywords.

### Defaults

No default behavior or values

### Command Modes

EXEC

### Examples

```
console# show statistics tacacs
TACACS+ Statistics
-----------------
Number of access requests: 0
Number of access deny responses: 0
Number of access allow responses: 0
```

### Related Commands

**authentication**

**show authentication**

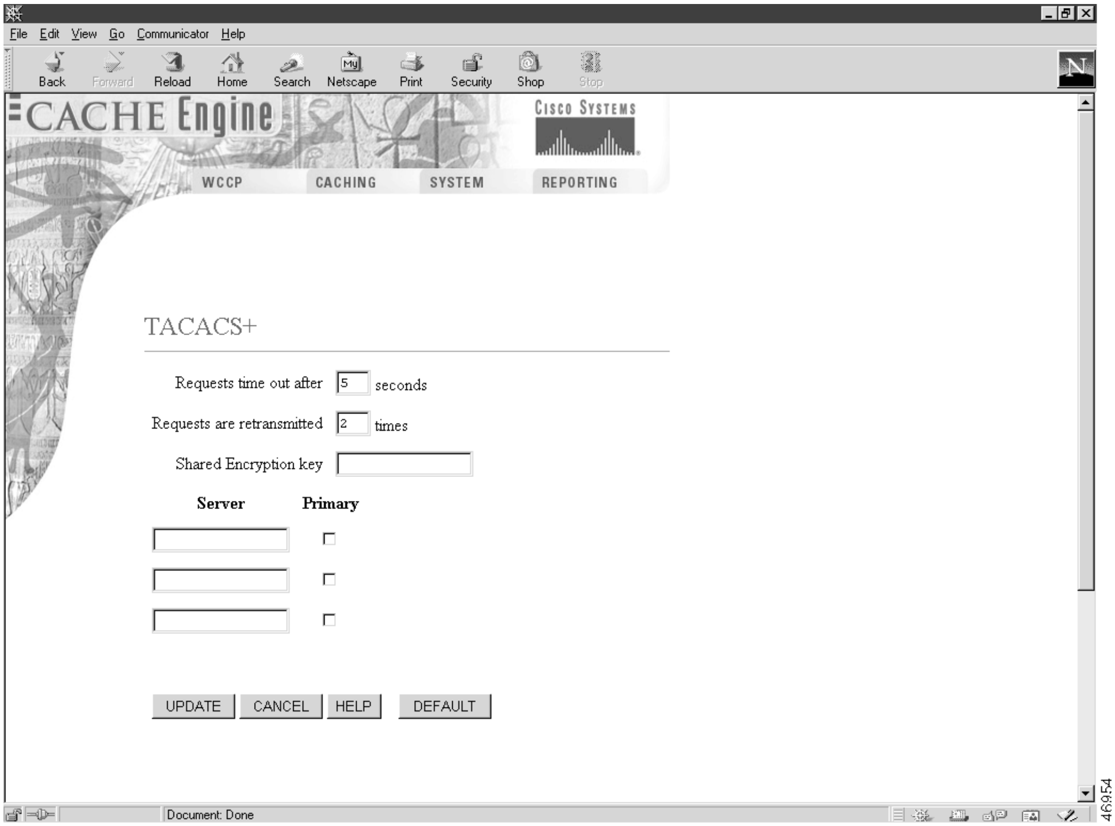
**show tacacs**

**tacacs**

## TACACS+ Page

The TACACS+ page has been added to the Systems menu. See the TACACS+ online help for further information.

*Figure 4 Management GUI—TACACS+ Page*


File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
CACHE Engine
Cisco Systems
WCCP CACHING SYSTEM REPORTING
UPDATE CANCEL HELP DEFAULT
Document: Done
46954

TACACS+

Requests time out after 5 seconds

Requests are retransmitted 2 times

Shared Encryption key

| Server | Primary |
|---|---|
|  | □ |
|  | □ |
|  | □ |

# Open Caveats

The following sections describe caveats still open at the printing of these release notes. Caveats describe unexpected behavior in the Cisco Cache software.

## Open Caveats—Software Release 2.3.0

- CSCds53244

  Symptom: When the number of active RADIUS authentication requests exceeds 950, requests that have recently been authenticated by the RADIUS server are forced to reauthenticate even though the authentication timeout interval defined by the **radius-server authtimeout** global configuration command has not expired.

  Possible cause: User entries in the RADIUS authentication cache in local CE RAM are not being purged properly. When the authentication cache is full, entries for recently authenticated users cannot be written to the authentication cache, forcing those users to reauthenticate on each attempt to access restricted content.

  When the CE authenticates a user through the RADIUS server, a record of that authentication is stored locally in the CE RAM. As long as the authentication entry is kept, subsequent attempts to access restricted content by that user do not require RADIUS server lookups. Entries are purged when they are inactive for a period defined by the authentication timeout interval.

  Workaround: There is no workaround, but power cycling the CE clears RAM contents, including the RADIUS authentication cache.

  Further information: This caveat will be resolved in Cache software, Release 2.3.1.

- CSCds54911

  Symptom: In some cases, Websense blocking messages for blocked requests are not returned to the client from a Websense server.

  Workaround: Ensure that the IP address and host name of the machine running the Websense server are specified in the internal Domain Name System (DNS) servers, or in the websense.ini file. To edit the websense.ini file, complete the following procedure:

**Step 1** Go to the Websense directory on the Websense server host.

**Step 2** Stop the Websense server.

**Step 3** Open the websense.ini file in a text editor.

**Step 4** In the [OpenServer] field of the websense.ini file, enter the following command on a blank line:

BlockPageServerName = <IP address>

where <IP address> is the IP address or host name of the computer running the Websense server.

**Step 5** Save the edited websense.ini file.

**Step 6** Restart the Websense server.

# Resolved Caveats

The following section describes caveats from previous releases that are resolved in Release 2.3.0.

- CSCdr13225

  Cisco Systems has observed that in topologies with 20 or more routers configured to service multiple Cache Engines, some of the Cache Engines do not receive hash allotments, and thus receive no redirected traffic from the routers. The routers can be configured in either unicast or multicast mode.

  Workaround: To correct this condition, reboot each Cache Engine or stop and start the Web Cache Communication Protocol (WCCP) on each Cache Engine using the Cache Engine **wccp** global configuration command.

  For example, to reset WCCP on a Cache Engine in the cache farm configured with basic web caching only, issue the following commands:

  ```
  console(config)# no wccp web-cache
  console(config)# wccp web-cache router-list 1
  ```

  Wait 30 seconds between stopping and starting WCCP. The **wccp** keywords and options shown here apply only to the Cache Engine in this example. Use the keywords and options appropriate to the configuration of each Cache Engine.

  Display the hash allotments for Cache Engines by using the **show ip wccp web-cache detail** router command.

- CSCdr23275

  The **http proxy outgoing exclude list** command is currently case sensitive. If a user on Netscape attempts to connect to HOME.INTERNAL.DOMAIN.COM, or Home.Internal.DOMAIN.Com, or any other combination of domain.com that is not all lowercase, then the **exclude list domain.com** command fails.

- CSCdr28820

  In certain cases, Java or JavaScript programs that run on port 80 are reset. The error bypass mechanism (in Cache Engine) fails to insert the correct IP address into the bypass list. Because the bypass list was not correctly updated, the Java or JavaScript traffic on port 80 was never bypassed.

- CSCdr38222

  Sometimes the BUCKET_IN flag is not cleared even though the corresponding AWAY flag is cleared in the Cache Engine that previously had the bucket.

- CSCdr47024

  When the Cache Engine is in bypass mode, with buckets bypassed, issuing the **no load bypass enable** command does not disable the bypass mechanism, and thus buckets stay bypassed.

- CSCdr51262

  When the origin server sends a large object with the wrong Content Length value, the Cache Engine deletes the object after downloading it. If there are multiple requests for the same object, the remaining clients receive a truncated object after the object is deleted.

- CSCdp64946

  When CEs are clustered and WCCP weights are changed dynamically, authenticated HTTP traffic may sometimes not be bypassed, though the authentication bypass feature is enabled (**bypass auth-traffic enable**).

- CSCdr89649

Specifying 65535 as an HTTPS destination port causes a page fault error.
(For example, **https destination-port allow 65535**, and **https destination-port deny 65535**). This has been fixed in the first post-FCS revision of release 2.2.0

# Related Documentation

*Cisco Content Engine 500 Series Hardware Installation Guide*

*Site Preparation and Safety Guide*

*Cisco Cache Software Configuration Guide*

*Cisco Cache Software Command Reference, Release 2.3.0*

Release Notes for the Cisco Content Engine or Cisco Cache Engine

Regulatory Compliance and Safety Information for the Cisco Content Engine or Cisco Cache Engine

# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the Web,  e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
    - From North America, call 408 526-8070
    - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

| Language | E-mail Address |
|---|---|
| English | tac@cisco.com |
| Hanzi (Chinese) | chinese-tac@cisco.com |
| Kanji (Japanese) | japan-tac@cisco.com |
| Hangul (Korean) | korea-tac@cisco.com |
| Spanish | tac@cisco.com |
| Thai | thai-tac@cisco.com |

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

# Obtaining Documentation

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco’s corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.