



Configuring Primary and Backup Proxy Servers for Standalone Content Engines

This chapter describes how to configure primary and backup (failover) proxy servers for standalone Content Engines that are running ACNS software, Release 5.2 or later.

This chapter contains the following sections:

- [Configuring Primary Proxy Failover, page 13-2](#)
- [Designating a Primary Outgoing HTTP Proxy Server, page 13-3](#)
- [Designating a Primary Outgoing FTP Proxy Server, page 13-3](#)
- [Designating a Primary Outgoing HTTPS Proxy Server, page 13-4](#)
- [Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings, page 13-5](#)
- [Monitoring Outgoing Proxy Servers and Statistics, page 13-7](#)
- [Displaying the Current Outgoing Proxy Server Configuration, page 13-8](#)
- [Displaying Outgoing Proxy Server Statistics, page 13-8](#)



Note

For complete syntax and usage information for the CLI commands used in this chapter, refer to the *Cisco ACNS Software Command Reference, Release 5.2* publication.

For information about configuring primary and backup proxy servers for Content Engines that are registered with a Content Distribution Manager, refer to the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*.

Configuring Primary Proxy Failover

For HTTP proxy caching, there is a primary proxy failover option that you can configure on standalone Content Engines. This feature is referred to as the HTTP proxy failover feature. With this feature, you can configure the forward proxy server to contact up to eight other proxy servers (outgoing proxy servers) when an HTTP cache miss occurs (that is, when the requested HTTP content is not already stored locally in the Content Engine cache).

You can use the **http proxy outgoing** global configuration command to configure up to eight backup Content Engines or any standard proxy servers for the HTTP proxy failover feature. These outgoing proxy servers can be other Content Engines or standard proxy servers that can be contacted to process HTTP cache misses without using ICP or WCCP. The function of these outgoing proxy servers is to process the HTTP cache misses that have been forwarded to them by the forwarding proxy server. One outgoing proxy server functions as the primary server to receive and process all cache miss traffic.

If the primary outgoing proxy server fails to respond to the HTTP request, the server is noted as failed and the requests are redirected to the next outgoing proxy server until one of the proxies services the request.

Failover occurs in the order that the proxy servers were configured. If all of the configured proxy servers fail, the Content Engine can optionally redirect HTTP requests to the origin server specified in the HTTP header if you have used the **http proxy outgoing origin-server** global configuration command. If the **origin-server** option is not enabled, the client receives an error message. Response errors and read errors are returned to the client, because it is not possible to detect whether these errors are generated at the origin server or at the proxy.



Note

At any one time, the Content Engine uses only one of the configured outgoing proxy servers. They cannot be used simultaneously. The state of the outgoing HTTP proxy servers can be viewed in syslog NOTICE messages and with the **show http proxy EXEC** command.

By default, the Content Engine strips the hop-to-hop 407 (Proxy Authentication Required) error code sent by the Internet proxy. If you issue the **http proxy outgoing preserve-407** global configuration command on a standalone Content Engine, the Content Engine sends the 407 error code to the requesting client browser, and the Internet proxy authenticates the client.

Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** global configuration command bypass the primary outgoing proxy server and the failover proxy servers.

If all of the outgoing proxy servers fail to process the HTTP cache miss, the following occurs:

- If the **http proxy outgoing origin-server** option is enabled, then the Content Engine (forward proxy server) forwards the HTTP cache miss request to the origin server that was specified in the original HTTP request from the client browser.
- If the **http proxy outgoing origin-server** option is not enabled, an error is sent to the requesting client browser. Response errors and read errors are returned to the requesting client browser, because it is not possible to detect whether these errors are generated at the origin server or at the proxy server.



Note

In ACNS software, Release 5.1 and earlier, the primary proxy failover feature supported HTTP only, not HTTPS or FTP. In ACNS 5.2 software, support for HTTPS-over-HTTP and FTP-over-HTTP was added.

The **no http proxy outgoing connection-timeout** option causes the timeout to be set to the default value of 300 milliseconds.

In this example, the Content Engine is configured to redirect HTTP requests directly to the origin server if all of the proxy servers fail.

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

Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** global configuration command bypass the primary outgoing proxy and the failover proxy servers.

Designating a Primary Outgoing HTTP Proxy Server

To configure a standalone Content Engine to direct all HTTP miss traffic to a parent cache without using the Internet Cache Protocol (ICP) or WCCP, you must explicitly designate a proxy server as the primary outgoing HTTP proxy server for the Content Engine.

Use the **http proxy outgoing host *host port primary*** global configuration command to designate a proxy server as the primary outgoing HTTP proxy server for the Content Engine, where:

- *host* is the host name or IP address of the outgoing HTTP proxy server.
- *port* is the port number designated by the outgoing (upstream) HTTP server to accept proxy requests.

Use the **primary** keyword to set the specified host as the primary outgoing HTTP proxy server. If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing HTTP proxy server for the Content Engine.

In this example, host 10.1.1.1 on port 8088 is explicitly designated as the primary outgoing HTTP proxy server for Content Engine A. Host 10.1.1.2 is configured as a backup outgoing HTTP proxy server.

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

**Note**

At any one time, the Content Engine uses only one of the configured outgoing HTTP proxy servers. They cannot be used simultaneously.

Designating a Primary Outgoing FTP Proxy Server

In ACNS 5.2 software, the ability to configure up to eight proxy servers for FTP miss traffic (FTP-over-HTTP) was added.

**Note**

At any one time, the Content Engine uses only one of the configured outgoing FTP proxy servers. They cannot be used simultaneously.

To configure a standalone Content Engine to direct all FTP-over-HTTP miss traffic to a parent cache without using ICP or WCCP, you must explicitly designate the parent cache as the primary outgoing FTP proxy server for the Content Engine.

Use the **ftp proxy outgoing host *host port primary*** global configuration command to designate a proxy server as the primary outgoing FTP proxy server for the Content Engine, where:

- *host* is the host name or IP address of the parent cache (the outgoing FTP proxy server) to which FTP missed traffic is directed.
- *port* is the port number used by the parent cache to accept missed FTP-over-HTTP requests from the Content Engine.

Use the **primary** keyword to set the specified host as the primary outgoing FTP proxy server. If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing FTP proxy server for the Content Engine.

In this example, host 10.1.1.1 on port 8088 is explicitly designated as the primary outgoing FTP proxy server for Content Engine A. Host 10.1.1.2 is configured as a backup outgoing FTP proxy server.

```
ContentEngineA(config)# ftp proxy outgoing host 10.1.1.1 8088 primary
ContentEngineA(config)# ftp proxy outgoing host 10.1.1.2 220
```

Designating a Primary Outgoing HTTPS Proxy Server

In ACNS software, Releases 5.1.x and earlier, you could only configure the Content Engine to use one outgoing HTTPS proxy server. In ACNS 5.2 software, the ability to configure up to eight HTTPS outgoing proxy servers for each Content Engine was added.



Note

At any one time, the Content Engine uses only one of the configured outgoing HTTPS proxy servers. They cannot be used simultaneously.

To configure a standalone Content Engine to direct all HTTPS miss traffic (HTTPS-over-HTTP) to a parent cache without using ICP or WCCP, you must explicitly designate a proxy server as the primary outgoing HTTPS proxy server for the Content Engine.

Use the **https proxy outgoing port primary** global configuration command to designate a proxy server as the primary outgoing HTTPS proxy server for the Content Engine, where:

- *host* is the hostname or IP address of the parent cache (outgoing HTTPS proxy server) to which HTTPS missed traffic is directed.
- *port* is the port number used by the parent cache to accept missed HTTPS-over-HTTP requests from the Content Engine.

Use the **primary** keyword to set the specified host as the primary outgoing HTTPS proxy server. If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing HTTPS proxy server for the Content Engine.

In this example, Content Engine A is configured to send its missed HTTPS traffic (that is, cache misses for browser requests for HTTPS content [HTTPS-over-HTTP requests]) to the host 10.1.1.1 on port 8088. Host 10.1.1.1 is explicitly designated as the primary outgoing HTTPS proxy server for Content Engine A. Host 10.1.1.2 is configured as a backup outgoing HTTPS proxy server for Content Engine A.

```
ContentEngineA(config)# https proxy outgoing host 10.1.1.1 8088 primary
ContentEngineA(config)# https proxy outgoing host 10.1.1.2 220
```

Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings

Certain scenarios involve the deployment of a Content Engine in proxy mode at company headquarters and Content Engines in transparent mode at remote locations in branch offices. In this scenario if a cache miss occurs at the remote Content Engine, company policy requires that the request be routed to the Content Engine at headquarters.

When an HTTP request intended for another proxy server is intercepted by the Content Engine in transparent mode, the Content Engine forwards the request to the intended proxy server if the **proxy-protocols transparent original-proxy** global configuration command was entered. If this command was not entered, then the Content Engine forwards the request directly to the origin server.

When the Content Engine is operating in transparent mode, it can intercept requests that were sent to another proxy server and send these requests to one of the following two destinations:

- **Default server**—This is the default option. The Content Engine retrieves the objects from the origin server itself, or if it is configured to use an outgoing proxy server for this protocol, it forwards the request to the specified outgoing proxy server. In this scenario, the client browser configuration is ignored, and the Content Engine configuration is used to retrieve the object from the server.
- **Original proxy**—The Content Engine forwards the request to the proxy server that the client originally addressed the request to. This may be different from the Content Engine's own outgoing proxy server for the specified protocol.

ACNS 5.x software also has an option that allows you to specify a single domain name, host name, or IP address to be globally excluded from proxy forwarding. The wildcard character * (asterisk) can be used for IP addresses (for instance, 172.16.*.*).



Note Requests with a destination specified with wildcard characters bypass the Content Engine proxy as well as the failover proxies.

The Content Engine addresses the request to the destination server directly and not to the client's intended proxy server.

When a Content Engine intercepts a proxy request intended for another proxy server and there is no outgoing proxy server configured for HTTPS-over-HTTP, and the **proxy-protocols transparent default-server** global configuration command is configured, the Content Engine addresses the request to the destination server directly and not to the client's intended proxy server.

However, all transparently intercepted requests sent by clients are returned to the client and requested objects are not delivered if the following two conditions exist:

- The **proxy-protocols transparent reset** command is configured on the Content Engine.
- A cache miss occurs.

You can use the Content Engine GUI or the CLI to configure HTTP and HTTPS outgoing proxy exclusion settings.

- From the Content Engine GUI, choose **Caching > Proxy Protocols**. Use the displayed Proxy Protocols window to configure these settings for this standalone Content Engine. For more information about how to use the Proxy Protocols window, click the **HELP** button in the window.
- From the Content Engine CLI, use the **proxy-protocols** global configuration commands. See [Table 13-1](#) and [Table 13-2](#). The order in which the CLI commands are entered is not important.

Table 13-1 Proxy Protocols Key Parameters

Key Content Engine GUI Parameter	Description	Corresponding Content Engine CLI Command
Default server	Specifies that the Content Engine should retrieve objects from the origin server itself. With this option, a proxy-style request can be sent to an outgoing proxy server if such a server is configured.	proxy-protocols transparent default-server
Original Proxy	Specifies that the Content Engine should forward the request to the original proxy addressed in the client request.	proxy-protocols transparent original-proxy
Do not use Outgoing Proxy for the following domains	Excludes the domain name, host name, or IP address specified here from proxy forwarding.	proxy-protocols outgoing proxy-exclude

Use the **proxy-protocols** global configuration command to specify a domain name, host name, or IP address to be excluded from proxy forwarding. To selectively turn off outgoing-proxy exclude lists or to force transparently received proxy-style requests to be fulfilled by the Content Engine, use the **no** form of this command.

proxy-protocols outgoing-proxy exclude {enable | list word}

proxy-protocols transparent {default-server | original-proxy | reset}

Table 13-2 describes the parameters for the **proxy-protocols** command.

Table 13-2 Parameters for the proxy-protocols Command

Parameter	Description
outgoing-proxy exclude	Sets global outgoing proxy exclude criteria.
enable	Enables global outgoing proxy exceptions.
list	Sets the global outgoing proxy exclude list.
<i>word</i>	Domain names, host names, or IP addresses to be excluded from proxy forwarding (supports 64 exclude list entries).
transparent	Sets transparent mode behavior for proxy requests.
default-server	Uses the Content Engine to go to the origin server or the outgoing proxy server, if configured.
original-proxy	Uses the intended proxy server from the original request.
reset	Resets the incoming connection.

The **proxy-protocols outgoing-proxy exclude** option allows you to specify a single domain name, host name, or IP address to be globally excluded from proxy forwarding. For example, if you enter the domain name `cisco.com`, then the configured outgoing proxy server will be bypassed each time the Content Engine tries to retrieve a web page from `cisco.com`. You can specify IP addresses instead of domain names. The wildcard character (*) can also be specified for IP addresses (for instance, `174.12.*.*`). You must press the **Enter** key after entering each local domain.

Domains are entered as an ASCII string, separated by spaces. The wildcard character * (asterisk) can be used for IP addresses (for instance, 172.16.*.*). Only one exclusion can be entered per command line. Enter successive command lines to specify multiple exclusions. Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** command bypass the Content Engine proxy as well as the failover proxy servers.

When you enter the **proxy-protocols transparent default-server** global configuration command, the Content Engine forwards intercepted HTTP, HTTPS-over-HTTP, and FTP-over-HTTP requests to the corresponding outgoing proxy server, if one is configured on the Content Engine. If no outgoing proxy server is configured for the protocol, the request is serviced by the Content Engine and the origin server.

The **proxy-protocols transparent original-proxy** option specifies that requests sent by a web client to another proxy server, but intercepted by the Content Engine in transparent mode, be directed back to the intended proxy server.

The **proxy-protocols transparent reset** option specifies that requests sent by a web client to another proxy server, but intercepted by the Content Engine in transparent mode, be returned to the web client during a cache miss. The requested objects are not delivered.

The following example configures the Content Engine to forward intercepted HTTPS-over-HTTP requests to an outgoing proxy server. The domain name cruzio.com is excluded from proxy forwarding.

```
ContentEngine(config)# https proxy outgoing host 172.16.10.10 266
ContentEngine(config)# proxy-protocols transparent default-server
ContentEngine(config)# proxy-protocols outgoing-proxy exclude list cruzio.com
```

The **show proxy-protocols EXEC** command verifies the configuration.

```
ContentEngine# show proxy-protocols all
Transparent mode forwarding policies: default-server
Outgoing proxy exclude list is enabled
Outgoing exclude domain name: cruzio.com
```

The following example configures the Content Engine to forward intercepted HTTP proxy-style requests to the intended proxy server.

```
ContentEngine(config)# proxy-protocols transparent original-proxy
```



Note

The MMS protocol can run on top of three different data protocols: MMS over TCP (MMST), MMS over UDP (MMSU), and MMS over HTTP.

Monitoring Outgoing Proxy Servers and Statistics

A background process on the Content Engine monitors the state of the configured outgoing proxy servers. You can configure the Content Engine to poll the specified outgoing proxy servers at a specific interval in order to monitor their availability.

This monitor interval is the frequency which the proxy servers are polled. The monitoring interval is specified in seconds, and can be from 10 to 300 seconds. The default monitoring interval is 60 seconds. If one of the outgoing proxy servers is unavailable, the polling mechanism waits for the connect timeout (300000 microseconds) before polling the next outgoing proxy server.

Use the following global configuration commands to specify the monitoring interval:

- Use the **http proxy outgoing monitor** command to specify how frequently the Content Engine polls the specified outgoing HTTP proxy servers.
- Use the **https proxy outgoing monitor** command to specify how frequently the Content Engine polls the specified outgoing HTTPS proxy servers.
- Use the **ftp proxy outgoing monitor** command to specify how frequently the Content Engine polls the specified outgoing FTP proxy servers.

In this example, the Content Engine is configured to monitor the outgoing HTTP proxy servers every 120 seconds.

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

You can also monitor outgoing proxy servers by checking the syslog NOTICE messages on the Content Engine.

Displaying the Current Outgoing Proxy Server Configuration

To display the Content Engine's current outgoing proxy server configuration, use the following EXEC commands:

- Use the **show http proxy** command to display the current outgoing HTTP proxy server configuration.
- Use the **show https proxy** command to display the current outgoing HTTPS proxy server configuration.
- Use the **show ftp proxy** command to display the current outgoing FTP proxy server configuration.

In this example, the **show http proxy** EXEC command is used to display the current configuration for outgoing HTTP proxy servers on the Content Engine.

```
ContentEngine# show http proxy
[/diamond/bin/exec_show_http] [proxy] [0x0]
Incoming Proxy-Mode:
  Configured Proxy mode HTTP connections on port: 2
Outgoing Proxy-Mode:
  Primary Proxy Server:           10.1.1.1 port 8088 Failed
  Backup Proxy Server:           1.1.1.1 port 1 Failed
Monitor Interval for Outgoing Proxy Servers is 120 seconds
Timeout period for probing Outgoing Proxy Servers is 1111 microseconds
Use of Origin Server upon Proxy Failures is disabled.
```

Displaying Outgoing Proxy Server Statistics

Use the **show statistics http proxy outgoing** EXEC command to display statistics about the HTTP requests that the Content Engine has sent to the specified HTTP proxy server.

```
ContentEngine# show statistics http proxy outgoing
HTTP Outgoing Proxy Statistics
```

IP	PORT	ATTEMPTS	FAILURES
10.1.1.1	8088	2396	2396
1.1.1.1	1	2396	2396