



## Content Engine GUI Menu Options

This appendix describes the tabs and subtabs (menu options), which are available from the Content Engine GUI. This is an alternative method that you can use to configure and monitor standalone Content Engines.

This appendix includes the following sections:

- [Content Engine GUI Tabs, page A-1](#)
- [WCCP Tab and Subtabs, page A-2](#)
- [Caching Tab and Subtabs, page A-3](#)
- [System Tab and Subtabs, page A-6](#)
- [Reporting Tab and Subtabs, page A-7](#)



**Note**

For information about how to access the Content Engine GUI, see the [“Logging in to the Content Engine GUI” section on page 3-54](#). The Content Engine GUI has context-sensitive help that can be accessed by clicking the **HELP** button at the bottom of the Content Engine GUI window.

## Content Engine GUI Tabs

[Table A-1](#) describes the four feature tabs and their associated functions.

**Table A-1**      *Content Engine GUI Feature Tabs*

Tab	Description
WCCP	Enables WCCP on the Content Engine and configures WCCP-related parameters and services (for example, configures the Content Engine to support the web cache service).
Caching	Configures cache-related parameters (for example, content preloading) on the Content Engine.
System	Configures system-related parameters (for example, access lists, DNS, and Websense server parameters) on the Content Engine.
Reporting	Displays statistics (for example, disk statistics, performance statistics, and WMT streaming statistics) gathered by the Content Engine.  Displays a hardware profile (model number, CPU, memory, disks, SCSI, and NICs) of the Content Engine, and the version of the ACNS software that is currently running on the Content Engine.

# WCCP Tab and Subtabs

Table A-2 lists the ACNS software, Release 5.1 or later features that can be configured from the WCCP tab and subtabs of the Content Engine GUI.

**Table A-2** Content Engine GUI WCCP Subtabs

Subtab Option	Description
<b>Enable WCCP</b>	Enables WCCP on the Content Engine. Use to enable WCCP Version 1 or WCCP Version 2 on the Content Engine.
<b>Clustering</b>	Sets parameters related to WCCP service clusters.
<b>Custom Web Cache</b>	(For WCCP Version 2 configuration only) Configures the WCCP custom web cache service on the Content Engine. When the Content Engine is configured to support this WCCP Version 2 service, it acts as a transparent forward proxy server for HTTP requests that are transparently redirected to it by any of the WCCP-enabled routers on the specified router list. If the requested content is not in its local cache, the Content Engine retrieves it from the origin web server, stores a local copy for future requests, and sends the client the requested content. Subsequent requests for the same content is served from the local cache on the Content Engine.
<b>Reverse Proxy</b>	(For WCCP Version 2 configuration only) Configures the WCCP reverse proxy service on the Content Engine. When the Content Engine is configured to support this WCCP Version 2 service, it acts as a reverse proxy; the Content Engine acts as a proxy on behalf of the origin web server.
<b>RTSP</b>	(For WCCP Version 2 configuration only) Configures the WCCP RTSP media cache service on the Content Engine (a transparent forward proxy server). The Content Engine listens for redirected RTSP requests on the standard RTSP port (default port 554). To configure the Content Engine to listen for intercepted RTSP requests on ports other than the default port (port 554), configure a user-defined WCCP service (services 90-97).  If the requested content is not in its local cache, the Content Engine retrieves it from the origin streaming server, stores a local copy for future requests, and sends the client the requested content. Subsequent requests for the same RTSP streaming content is served from the local cache on the Content Engine.
<b>Services</b>	(For WCCP Version 2 configuration only) Configures the Content Engine to cache web traffic using multiple ports, using the user-defined WCCP services (service 90 to 97). To configure these generic WCCP Version 2 services, use this WCCP Services window.

**Table A-2** Content Engine GUI WCCP Subtabs (continued)

Subtab Option	Description
Web Cache	<p>(WCCP Version 1 or Version 2 configuration)</p> <p>Configures the WCCP web-cache service (service 0) on the Content Engine (transparent forward proxy server). This service permits the Content Engine to accept transparently redirected HTTP requests on a single port (port 80). If the requested content is not in its local cache, the Content Engine retrieves it from the origin web server, stores a local copy for future requests, and sends the client the requested content. Subsequent requests for the same web content is served from the local cache on the Content Engine.</p> <p>Only a single WCCP router is supported with WCCP Version 1; whereas, multiple routers (router list) are supported with WCCP Version 2. To enable the Content Engine to listen for WCCP intercepted HTTP traffic on ports other than the default port, configure the custom-web-cache service or a user-defined WCCP service (services 90 to 97).</p>
WMT-Streaming	<p>(For WCCP Version 2 configuration only)</p> <p>Configures the WCCP WMT media caching service on the Content Engine (transparent forward proxy server). If the requested content is not in its local cache, the Content Engine retrieves it from the origin streaming server, stores a local copy for future requests, and sends the client the requested content. Subsequent requests for the same WMT streaming content is served from the local cache on the Content Engine.</p>

## Caching Tab and Subtabs

Table A-3 lists the ACNS software, Release 5.1 or later features that can be configured from the Caching tab and subtab of the Content Engine GUI.

**Table A-3** Content Engine GUI Caching Subtabs

Subtab Option	Description
Auth. Cache	Configures cache authentication on the Content Engine. For more information, see the <a href="#">“Configuring Authenticated HTTP Cache Settings”</a> section on page 6-11.
Bypass	<p>(For WCCP Version 2 configuration only)</p> <p>Configures bypass on the Content Engine. For more information, see the <a href="#">“Configuring Bypass Settings on Standalone Content Engines”</a> section on page 14-3.</p>
Cache on Abort	<p>Configures cache-on-abort features on the Content Engine. Determines the policy for object caching that the Content Engine should use if the web client aborts the download process.</p> <p>If this option is enabled, the Content Engine uses a selective algorithm to determine whether to continue to cache an object if the web client has aborted the download. If disabled, the Content Engine will always continue to download an object to the cache even if a web client has aborted the download.</p>
Content Preload	Configures content preloading on the Content Engine. For more information, see the <a href="#">“Configuring Content Preloading for Standalone Content Engines”</a> section on page 3-60.
Customized Error Page	Create HTTP customized error pages. If you create these customized pages, then the Content Engine displays the appropriate customized error page instead of the default error message when proxy errors occur. For more information, see the <a href="#">“Creating HTTP Custom Error Pages for Standalone Content Engines”</a> section on page 20-49.
FTP Freshness	View or configure FTP object freshness factors for the Content Engine. For more information, see the <a href="#">“About FTP Cache Freshness”</a> section on page 6-38.

Table A-3 Content Engine GUI Caching Subtabs (continued)

Subtab Option	Description
<b>FTP Proxy</b>	<p>Configures FTP incoming and outgoing proxies for the Content Engine. Proxy mode enables the Content Engine to operate in environments where WCCP is not enabled, or where client browsers have previously been configured to use a legacy FTP proxy server. DNS must be configured in order to support incoming FTP proxy requests.</p> <p>For more information, see the <a href="#">“Configuring FTP-over-HTTP Caching on Standalone Content Engines” section on page 6-41.</a></p>
<b>HTTP Freshness</b>	<p>View or configure freshness factors HTTP objects that are currently cached on the Content Engine. For more information, see the <a href="#">“Configuring HTTP Cache Freshness Settings” section on page 6-8.</a></p>
<b>HTTP Proxy</b>	<p>Configures HTTP incoming and outgoing proxies for the Content Engine. Proxy mode enables the Content Engine to operate in environments where Cisco’s WCCP is not enabled, or where client browsers have previously been configured to use a legacy proxy server. DNS must be configured in order to support incoming HTTP proxy requests.</p> <p>For more information, see the <a href="#">“Configuring Nontransparent HTTP Forward Proxy Caching on Standalone Content Engines” section on page 6-7.</a></p>
<b>HTTPS Proxy</b>	<p>Configures HTTPS incoming and outgoing proxies. HTTPS proxy mode enables the Content Engine to service HTTPS requests sent by web clients that are configured to use an HTTPS proxy server. DNS must be configured in order to support incoming HTTPS proxy requests.</p> <p>For more information, see the <a href="#">“Configuring HTTPS Proxy Caching for Standalone Content Engines” section on page 6-25.</a></p>
<b>ICP Client</b>	<p>Configures a Content Engine cluster to generate ICP queries before retrieving the requested objects from the Internet. For example, specify how long the Content Engine should wait before retrieving the needed data directly from the Internet. By default, the Content Engine waits for 2 seconds; however, you can change this default. The range is 1 to 30 seconds.</p> <p>For more information, see the <a href="#">“Configuring Standalone Content Engines as ICP Clients” section on page 6-57.</a></p>
<b>ICP Server</b>	<p>Configures a Content Engine to act as an ICP server. Specify whether the Content Engine is the parent server or sibling server for the designated ICP client. If the Content Engine is the parent ICP server and cannot satisfy the ICP client’s request, it forwards the request to another server on the Internet. If the Content Engine is a sibling ICP server and cannot satisfy the ICP client’s request, it will send a failed response back to the ICP client.</p> <p>For more information, see the <a href="#">“Configuring Standalone Content Engines as ICP Servers” section on page 6-58.</a></p>
<b>LDAP</b>	<p>Configures the Content Engine to use an LDAP server for authentication purposes. To enable the Content Engine to use a specific LDAP server, enter the IP address of the LDAP server, and the port number that the LDAP server will be listening on. The default LDAP port number is 389. LDAP authentication is not performed if no LDAP servers are configured.</p> <p>For more information, see the <a href="#">“Configuring LDAP Authentication of HTTP Requests” section on page 9-14.</a></p>

Table A-3 Content Engine GUI Caching Subtabs (continued)

Subtab Option	Description
<b>NTLM</b>	<p>Configures the Content Engine to use an NTLM server for authentication purposes. To enable the Content Engine to use a specific NTLM server, enter the host information. For example, specify the domain name (the domain name in which the user should be authenticated) and the domain server (the IP address or host name of the NTLM server). NTLM authentication will not be performed if no NTLM servers are configured.</p> <p>For more information, see the <a href="#">“Configuring NTLM Authentication of HTTP Requests”</a> section on page 9-29.</p>
<b>Persist. Connect.</b>	<p>Configures persistent connections on the Content Engine. Persistent connections can be set for <b>client-only</b>, <b>server-only</b>, and <b>all</b> connections on the Content Engine.</p> <p>If the <b>Strip NTLM Authentication headers</b> option is turned off in the Content Engine, the NTLM authentication headers will be sent to the client. The Content Engine will not support NTLM authentication if persistent connections for <b>all</b> is turned off.</p> <p>For more information, see the <a href="#">“Configuring Persistent Connections”</a> section on page 6-52.</p>
<b>Proxy Protocols</b>	<p>Configures proxy protocols for the Content Engine. The default behavior is that the Content Engine will retrieve the objects from the origin web server itself, or, if configured to use an outgoing proxy for this protocol, will forward the request to the specified outgoing proxy.</p>
<b>RADIUS</b>	<p>Configures the Content Engine to use a remote RADIUS server for authentication purposes. Configure the network parameters required to access the remote RADIUS database.</p>
<b>RealProxy</b>	<p>Enables the RealProxy GUI Administration page. Note that Real Proxy must be configured properly using the in order to start the Real Proxy.</p> <p>For more information about RealProxy, see the <a href="#">“Configuring RealProxy with the RealSystem Administrator GUI”</a> section on page 8-20.</p>
<b>Transaction Logs</b>	<p>Enable and configure transaction logging. By default, transaction logging is disabled. For more information, see the <a href="#">“Monitoring Transactions with Standalone Content Engines”</a> section on page 20-18.</p>
<b>URL Filtering</b>	<p>Configures URL filtering. For more information, see <a href="#">Chapter 10, “Configuring URL Filtering on Standalone Content Engines.”</a></p>
<b>WMT-Streaming</b>	<p>Enables WMT and configures WMT streaming parameters. For more information, see the <a href="#">“Configuring WMT Streaming and Caching Services for Standalone Content Engines”</a> section on page 7-10.</p>

# System Tab and Subtabs

Table A-4 lists the ACNS software, Release 5.1 or later features that can be configured from the System tab and subtabs of the Content Engine GUI.

**Table A-4** Content Engine GUI System Subtabs

Subtab Option	Description
<b>Access Lists</b>	Manage group name-based access lists on the Content Engine. In environments in which the Content Engine has been deployed as a standalone caching engine, you can use group-based access lists to control which groups of users can view specific content that is served by the Content Engine. For more information, see the <a href="#">“Configuring RADIUS Authentication of HTTP Requests”</a> section on page 9-11.
<b>Authentication</b>	Configure how the Content Engine is to authenticate and authorize administrative users. For more information, see <a href="#">Chapter 16, “Configuring Administrative Login Authentication and Authorization on Standalone Content Engines.”</a>
<b>Basic Networking</b>	Adjust the network settings (the default gateway and the hostname) for the Content Engine.
<b>CDP</b>	Configure the Cisco Discovery Protocol (CDP) for the Content Engine. By default, CDP is enabled on a Content Engine.
<b>DNS</b>	Configure DNS name servers for the Content Engine to use for domain name resolution, and enable DNS caching on the Content Engine. For more information about this topic, see the <a href="#">“Configuring Bandwidth for Interfaces and Content Services”</a> section on page 15-5.
<b>File System</b>	View information about the currently configured file systems.
<b>NTP</b>	Set the Content Engine time and date.
<b>Real Subscriber</b>	View Real Subscriber activities.
<b>Routing</b>	Use to add a new entry to the routing table.
<b>Rules Template</b>	Configure or modify a Rules Template on the Content Engine. For more information, see <a href="#">Chapter 12, “Configuring the Rules Template on Standalone Content Engines.”</a>
<b>SNMP</b>	Configure SNMP on the Content Engine. For more information, see the <a href="#">“Monitoring Standalone Content Engines with SNMP”</a> section on page 20-3.
<b>Syslog</b>	Configure the Content Engine to send varying levels of event messages to a syslog host. For more information, see the <a href="#">“Configuring System Logging on Standalone Content Engines”</a> section on page 20-44.
<b>TACACS+</b>	Configure the Content Engine to use a TACACS+ server for authentication and authorization. Configure the network parameters required to access the remote TACACS+ database. For more information, see the <a href="#">“Understanding TACACS+ Authentication and Authorization”</a> section on page 16-7.
<b>TCP</b>	Change the default TCP settings on the Content Engine. For more information, see <a href="#">Chapter 19, “Viewing and Modifying TCP Stack Parameters on Standalone Content Engines.”</a>
<b>Users</b>	Add, delete, or modify user accounts and privileges. These entries are stored in the local database that resides on the Content Engine. For more information, see <a href="#">Chapter 16, “Configuring Administrative Login Authentication and Authorization on Standalone Content Engines.”</a>
<b>Websense Server</b>	Use to start or stop the Websense server, and to view information about the local Websense server. For more information, see the <a href="#">“URL Filtering with Websense Software”</a> section on page 10-11.

# Reporting Tab and Subtabs

Table A-5 lists the statistics and other information that are accessible from the Reporting tab and subtabs of the Content Engine GUI.

**Table A-5** Content Engine GUI Reporting Subtabs

Subtab Option	Description
<b>Disk Stats</b>	View general CFS disk statistics for the Content Engine.
<b>Hardware Info</b>	View detailed information about the Content Engine hardware components (for example, model number and RAM size).
<b>IMS Stats</b>	View If-Modified-Since (IMS) request activity (for example, the total number of requests from clients to the Content Engine).
<b>Java Monitor</b>	Monitor the Content Engine resources; obtain a graphical depiction of Content Engine utilization.
<b>Performance</b>	View performance statistics for the Content Engine.
<b>Request</b>	View statistics on miscellaneous HTTP request data (for example, the number of forced reloads).
<b>Savings</b>	View the number of requests that have been served by the Content Engine.
<b>TCP</b>	View the amount of requests that have been served by the Content Engine.
<b>Usage</b>	View the resource utilization statistics for the Content Engine.
<b>WMT-Streaming</b>	View WMT streaming statistics.

