



Configuring Request Authentication and Authorization

This chapter explains how to configure request authentication and authorization for centrally managed ACNS networks. It contains the following sections:

- [Understanding Request Authentication and Authorization, page 13-1](#)
- [Configuring Request Authentication, page 13-3](#)



Note

Content request authentication and authorization is independent of login (user) authentication and authorization. For information about login authentication and authorization, see [Chapter 14, “Configuring Login Authentication, Configuration Authorization and Accounting.”](#)

Understanding Request Authentication and Authorization

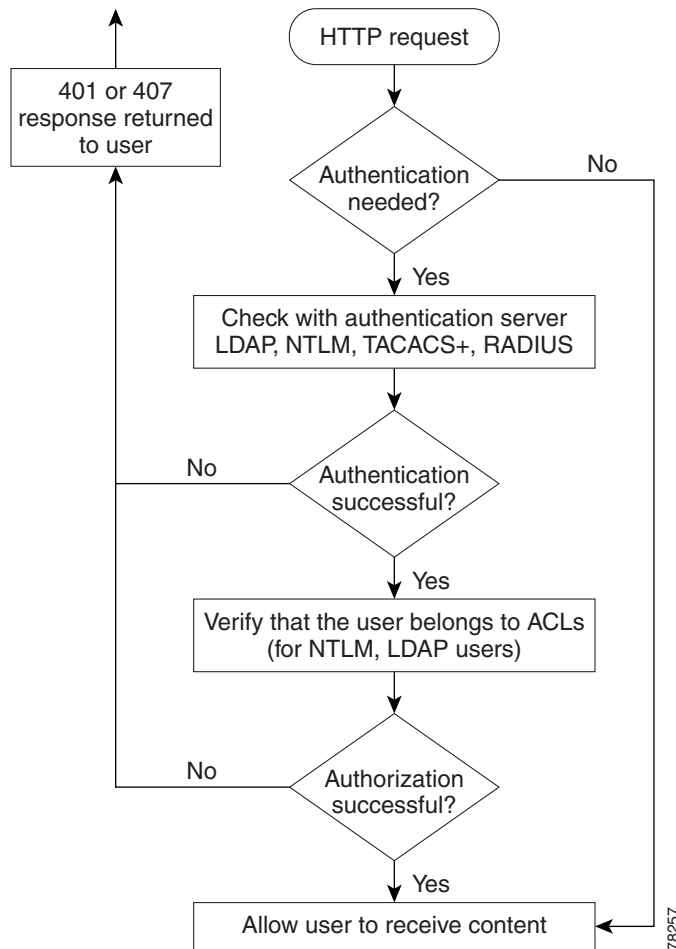
As organizations extend the use of web applications and Internet access to their employees, they are confronted with the following challenges:

- How to manage employee use of the Internet
- How to restrict access to online content

Organizations can use request authentication and authorization to address these concerns. For example, organizations can use HTTP request authentication as a mechanism to restrict access to online content. If HTTP authentication is configured on a Content Engine, the Content Engine checks a remote database (for example, a RADIUS, TACACS+, LDAP, or NTLM database) for user password authentication to determine if the user should be granted or denied access to the requested content.

For more granular control, organizations can use group-based authorization (for NTLM and LDAP users) in addition to HTTP authentication. If the Content Engine is configured for group-based authorization, then the Content Engine checks its access control lists (ACLs) to determine if the group that the user belongs to should be granted or denied access to the requested content. [Figure 13-1](#) shows how HTTP request authentication and group-based authorization can be used as mechanisms to control access to content.

Figure 13-1 HTTP Request Authentication and Group-Based Authorization

**Note**

Note that group-based authorization occurs only after HTTP request authentication has occurred.

About HTTP Request Authentication

ACNS 5.x software supports TACACS+, NTLM, LDAP, and RADIUS servers for HTTP request authentication. In the case of NTLM, HTTP request authentication authenticates a user's domain, username, and password with a preconfigured primary domain controller (PDC) before allowing requests from the user to be served by the Content Engine.

With an HTTP query, the Content Engine obtains a set of credentials from the user (user ID and password) and compares them against those in the authentication server database. When the Content Engine authenticates a user through an authentication server, a record of that authentication is stored locally in the Content Engine RAM (authentication cache). As long as the authentication entry is kept, subsequent attempts to access restricted Internet content by that user do not require authentication server lookups.

The Content Engine supports HTTP request authentication for both proxy mode and transparent (WCCP) mode access.

- In proxy mode, the Content Engine uses the client's user ID as a key for the Content Engine's authentication cache.
- In transparent mode, the Content Engine uses the client's IP address as a key for the Content Engine's authentication cache.

If you are using HTTP request authentication in transparent mode, we recommend that the AuthTimeout interval configured with the **http authentication cache timeout** command be short. IP addresses can be reallocated, or different users can access the Internet through an already authenticated device (PC, workstation, and the like). Shorter AuthTimeout values help reduce the possibility that individuals can gain access using previously authenticated devices. When the Content Engine operates in proxy mode, it can authenticate the end user with the user ID and password.

The default time interval between the user's last Internet access and the removal of that user's entry from the authorization cache is 480 minutes. The minimum time interval is 1 minute, and the maximum is 1440 minutes (24 hours). The Content Engine forces reauthentication with the authentication server once this time interval expires.

Configuring Request Authentication

This section outlines the requirements for the Content Distribution Manager authentication and authorization management system and the integration with back-end access control servers.

To configure request authentication on the Content Engine, you must complete the following tasks:

1. Determine which one of the supported external authentication servers that you want the device to use when authenticating content requests.
2. Configure the authentication server settings that you wish to use on the Content Engine. (See the next section, "[Configuring Authentication Server Settings](#).")
3. Specify which authentication database the device should check to process the request authentication. (See the "[Setting the Authentication Scheme for Request Authentication](#)" section on page 13-13.)

Configuring Authentication Server Settings

Some Cisco ACNS network users use an external access server as a centralized location for controlling the authentication, authorization, and accounting of user accounts and activities. External authentication servers are implemented at the protocol and application level with TACACS+, RADIUS, LDAP, and NTLM.

Only one type of request authentication can be enabled at a time. For example, you cannot enable both LDAP authentication and NTLM authentication at the same time.

This section describes how to configure LDAP, NTLM, RADIUS, and TACACS+ server settings for the Content Engine.

Configuring LDAP Server Settings

System administrators can use the Content Engine to restrict user Internet access using an LDAP server for authentication purposes. ACNS 5.x software supports LDAP Version 2 and Version 3 and supports all LDAP features except for Secure Authentication and Security Layer (SASL).

To configure LDAP server settings using the Content Distribution Manager GUI, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the name of the Content Engine that you want to configure. The Contents pane appears on the left.
- Step 3** From the Contents pane, choose **General Settings > Authentication > LDAP Server**. The LDAP Server Settings window appears. (See Figure 13-2.) Table 13-1 describes the fields shown in this window.

Figure 13-2 LDAP Server Settings Window

The screenshot shows the 'LDAP Server Settings for Content Engine, CONTENTENGINE' window. The 'Contents' pane on the left is expanded to 'Authentication > LDAP Server'. The main area shows the following fields:

- Current settings: None (Using Factory Defaults)
- Enable LDAP Servers *:
- LDAP Version: * dropdown menu (version 2)
- Time to wait: * text input field
- Number of Retransmits: * text input field
- User-id Attribute: * text input field
- Filter: text input field
- Base Distinguished Name: * text input field
- Administrative DN: text input field
- Administrative DN Password: text input field
- Confirm Password: text input field
- Allow-Mode:
- Active Directory Groups:
- Server Port: * text input field
- Primary Host: * text input field
- Secondary Host: text input field

* To use LDAP for Request Authentication, please go to the Authentication Scheme Settings page.

Note: * - Required Field

Buttons: Submit, Cancel

- Step 4** Check the **Enable LDAP Servers** check box.
- Step 5** From the LDAP Version drop-down list, choose the LDAP protocol version to be used.
- Step 6** In the Time to wait field, specify the number of seconds that the Content Engine waits before timing out.
- Step 7** In the Number of Retransmits field, specify the number of times that the Content Engine can try to reestablish its connection to the LDAP server if the timeout value is exceeded while it tries to contact the LDAP server. The number of transmission attempts can be from 1 to 3. The default is two attempts.
- Step 8** In the User-id Attribute field, enter the user ID attribute.
- Step 9** In the Filter field, enter the filter string to be used by the LDAP server.
- Step 10** In the Base Distinguished Name field, enter the base distinguished name string for the search in the LDAP server.
- Step 11** In the Administrative DN field, enter the administrative distinguished name.
- Step 12** In the Administrative DN password field, enter the administrative distinguished name password.

- Step 13** Check the **Allow-Mode** check box to enable access to users when the LDAP server is unavailable.
- Step 14** Check the **Active Directory Groups** check box to allow the use of Windows Active Directory groups.
- Step 15** In the Server Port field, specify a TCP port number for LDAP server authentication. We suggest using the default port value of 389.
- Step 16** Enter the IP address of the primary LDAP server in the Primary Host field.
- Step 17** Enter the IP address of the secondary LDAP server in the Secondary Host field.
- Step 18** Click **Submit** to save the settings.

Table 13-1 LDAP Server Settings

GUI Parameter	Function	CLI Command
Enable LDAP Servers	Enables HTTP authentication using LDAP servers.	ldap server enable
LDAP Version	LDAP protocol version (Version 2 or Version 3) to be used.	ldap server version
Time to wait	Number of seconds that the Content Engine waits for a response before timing out on a connection to a particular LDAP server. The default value is 5 seconds.	ldap server timeout
Number of Retransmits	Number of attempts allowed to connect to an LDAP server. The default value is 2 times.	ldap server retransmit
User-id Attribute	Name of the user ID attribute on the LDAP server. The default is "uid."	ldap server userid-attribute
Filter	LDAP filter string. There is no default value.	ldap server filter
Base Distinguished Name	Base distinguished name of the starting point for the search of the LDAP server. This allows for a search on a particular string, such as the domain "com."	ldap server base
Administrative DN	Administrative distinguished name. Allows a search for a particular user associated with the base distinguished name.	ldap server administrative-dn
Administrative DN Password	Password for the administrative distinguished name.	ldap server administrative-passwd
Allow-Mode	Allows access to users when the LDAP server is unavailable.	ldap server allow-mode
Active Directory Group	Allows access to Windows Active Directory groups.	ldap server active-directory-group
Server Port	Port number on which the LDAP server is listening. The default port number is 389.	ldap server port
Primary Host	IP address of the primary LDAP server.	ldap server host
Secondary Host	IP address of the secondary LDAP server.	ldap server host

Configuring NTLM Server Settings

The NTLM protocol can be used to authenticate and block user access to the Internet. When a user logs in to a Windows NT or a Windows 2000 domain and starts a browser, the authentication information is stored by the browser and later used as NTLM credentials to access the Internet. The browser sends the NTLM credentials with the domain name to the ACNS software cache, which in turn sends a request to the Windows NT domain controller to check the validity of the user in the domain. If the user is not a valid user in the domain, then the request to access the Internet is denied. If authentication succeeds, the source IP address is entered in the authentication cache. Future requests from this IP address are not challenged until the authentication cache entry expires or is cleared.

Before invoking an NTLM authentication request, make sure that the following conditions exist:

- The NTLM primary domain controller (PDC) has an entry in the DNS that matches its NetBIOS-named computer account.
- The primary domain controller is both forward and reverse DNS-resolvable.
- The domain name configured on the Content Engine should be a domain that can be authenticated through the primary domain controller.

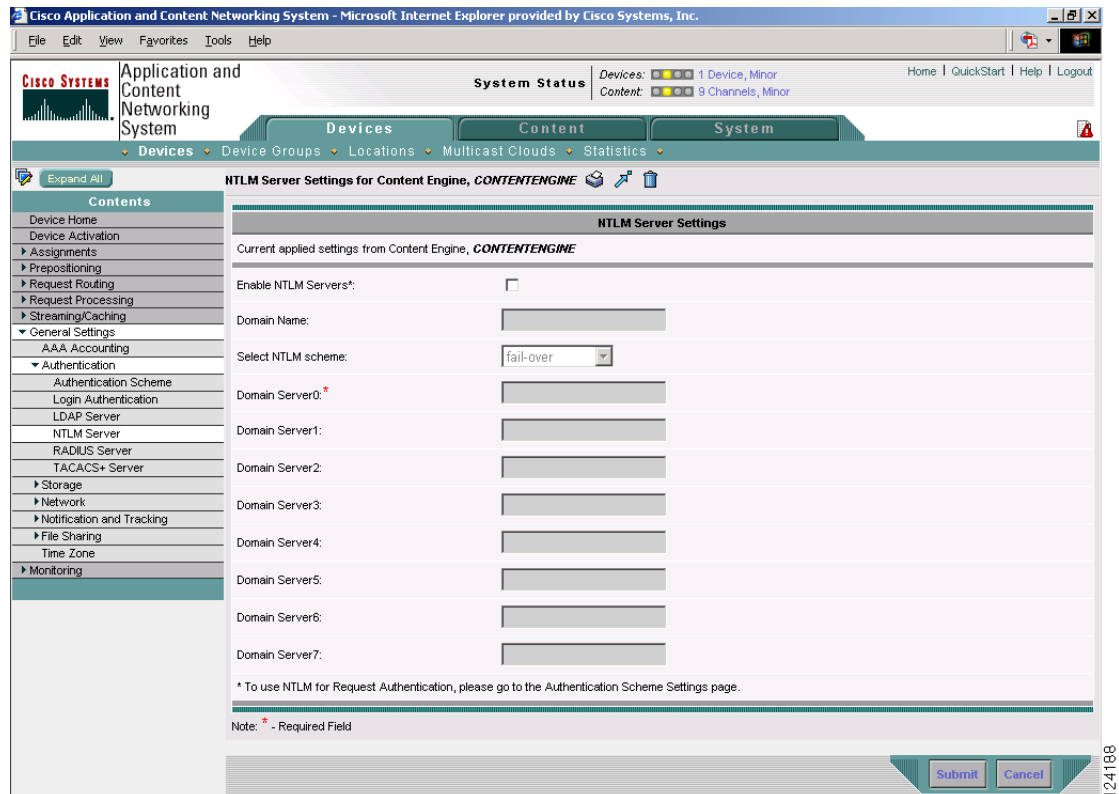
**Note**

This domain can be either a domain hosted by the PDC, or a trusted domain that the PDC can authenticate by contacting other PDCs.

To configure NTLM server settings using the Content Distribution Manager GUI, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
 - Step 2** Click the **Edit** icon next to the name of the Content Engine that you want to configure. The Contents pane appears on the left.
 - Step 3** From the Contents pane, choose **General Settings > Authentication > NTLM Server**. The NTLM Server Settings window appears. (See [Figure 13-3](#).) [Table 13-2](#) describes the fields shown in this window.

Figure 13-3 NTLM Server Settings Window



Step 4 Check the **Enable NTLM Servers** check box to enable NTLM authentication, configure the NTLM server domain name, NT primary domain controller name or IP address, and optionally set the host name or address as primary or secondary.

Before making an NTLM authentication request, make sure that the following conditions are met:

- The NTLM primary domain controller has an entry in the Domain Name System (DNS) that matches its NetBIOS-named computer account.
- The primary domain controller is both forward and reverse DNS-resolvable.
- The domain name configured on the Content Engine matches the domain of which the primary domain controller is a part. This domain can be either a domain hosted by the PDC, or a trusted domain that the PDC can authenticate by contacting other PDCs.

Step 5 In the Domain Name field, specify the domain name in which the user should be authenticated. (See the “[Support for No Default NTLM Domain](#)” section on page 13-8.)

Step 6 From the Select NTLM scheme drop-down list, choose an option to specify the scheme for the NTLM servers for HTTP request authentication. This option allows you to specify the scheme (load balancing or failover) that is to be used among the configured NTLM servers. The default scheme is **fail-over**; the other supported scheme is **load-balanced**.

When the load balancing scheme is enabled, only the first request is sent to the first configured server, and then round robin is used among the configured servers. (See the “[About NTLM Load Balancing for HTTP Request Authentication](#)” section on page 13-8.) When the failover scheme is enabled, the Content Engine sends all the requests to the first configured server. (See the “[About NTLM Failover for HTTP Request Authentication](#)” section on page 13-9.)

Step 7 In the Domain Server0 field, enter the host name or IP address for the domain server. The server configured as Server0 becomes the primary NTLM domain server when multiple servers are configured for failover purposes.

Step 8 In the Domain Server fields 1 through 7, enter the host names or IP addresses of each NTLM server that you want the Content Engine to use for HTTP request authentication. This list of configured NTLM servers is referred to as the “host list.”

In ACNS software, you can configure a Content Engine to use up to eight NTLM servers for HTTP request authentication. The order of the server configuration determines the order of load balancing or failover.

Step 9 Click **Submit** to save the settings.

Table 13-2 NTLM Server Settings

GUI Parameter	Function	CLI Command
Domain Name	Domain name in which the user should be authenticated.	ntlm server domain <i>name</i>
Select NTLM Scheme	Scheme for the NTLM servers for HTTP request authentication.	ntlm server scheme { fail-over load-balanced }
Domain Server0	NTLM server that serves as the primary host.	ntlm server host { <i>hostname</i> <i>ipaddress</i> } primary
Domain Server1–7	NTLM servers that serve as backup hosts.	ntlm server host { <i>hostname</i> <i>ipaddress</i> } secondary

Support for No Default NTLM Domain

ACNS software sends a “no domain configuration” error message to the client when the user does not supply a domain name in the request authentication credential and has not configured a default domain on the Content Engine. The error message contains text indicating the reason for the error.



Note

The no domain configuration feature is only supported with browsers that do not support NTLM (for example, Netscape browsers). For the Netscape browser, the user must specify the domain if the Content Engine does not have an NTLM default domain configured; otherwise the client receives an error. Note that for the Netscape browser, the domain can only be supplied as part of the username in the format of “domain\username.” Browsers that do support NTLM such as Internet Explorer always include a domain name in the authentication credentials that originate from either the user being prompted to specify the credentials or from the domain that was used to log the user on to their desktop.

About NTLM Load Balancing for HTTP Request Authentication

In large-scale networks where all network traffic passes through the Content Engine, even though the Content Engine authentication cache helps reduce the load on the domain controller, it might still be impractical to have a single domain controller handling all the authentication queries from end users. ACNS 5.2 software provides the ability to configure up to eight servers (domain controllers) for load balancing and failover purposes.

When you choose **load-balanced** as the authentication scheme, requests are round-robin among the domain controllers. The order in which the domain controllers (servers) are configured determines the order of load balancing. For example, if you have n servers, the first request is sent to Server 0 and the second request is sent to Server 1, the n th request is sent to Server $n - 1$ and the $n + 1$ request is sent to Server 0. If Server 0 fails, the Content Engine attempts to send the request to the next alive server (in this case, Server 1). However, failover to the next alive server occurs a maximum of one time. For example, if Server 1 goes down when handling request 1, then request 1 does not fail over again.

If load balancing is enabled and the server information is changed during run time, the change is picked up at run-time without disrupting the service.

About NTLM Failover for HTTP Request Authentication

ACNS 5.2 software supports failover between domain controllers. The order in which the domain controllers (servers) are configured determines the order of failover. The first server configured (Server 0) is the first server to be contacted. The last server configured (Server 7) is the last server to be contacted.

If the timeout period for one connection attempt is exceeded, the Content Engine drops the connection and attempts to reconnect to the same server. The Content Engine retries the connection up to the specified number of retries configured (**ntlm server connection-retry** global configuration command), before attempting to connect to the next configured server on the host list.

Configuring RADIUS Server Settings

RADIUS authentication clients reside on devices running ACNS 5.x software. When enabled, these clients send authentication requests to a central RADIUS server, which contains user authentication and network service access information.



Tip

The Content Distribution Manager does not cache the user authentication information. Therefore, the user is reauthenticated against the RADIUS server for every request. To prevent performance degradation caused by many authentication requests, install the Content Distribution Manager in the same location as the RADIUS server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure RADIUS server settings using the Content Distribution Manager GUI, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the name of the Content Engine that you want to configure. The Contents pane appears on the left.
- Step 3** From the Contents pane, choose **General Settings > Authentication > RADIUS Server**. The RADIUS Server Settings window appears. (See [Figure 13-4](#).) [Table 13-3](#) describes the fields in this window.

Figure 13-4 RADIUS Server Settings Window

The screenshot shows the 'RADIUS Server Settings' window for the Content Engine, CONTENTENGINE. The window is titled 'Cisco Application and Content Networking System - Microsoft Internet Explorer provided by Cisco Systems, Inc.' and includes a navigation menu on the left with options like 'Device Home', 'Assignments', 'Prepositioning', 'Request Routing', 'Request Processing', 'Streaming/Caching', 'General Settings', 'AAA Accounting', 'Authentication', 'Storage', 'Network', 'Notification and Tracking', 'File Sharing', 'Time Zone', and 'Monitoring'. The main content area is titled 'RADIUS Server Settings' and contains the following fields:

- Enable RADIUS Servers*:
- Time to wait: (Default: 5)
- Number of retransmits: (Default: 3)
- Enable Redirect:
- Redirect Message 1: Location 1:
- Redirect Message 2: Location 2:
- Redirect Message 3: Location 3:
- Shared Encryption Key:
- Server 1 Name: Server 1 Port:
- Server 2 Name: Server 2 Port:
- Server 3 Name: Server 3 Port:
- Server 4 Name: Server 4 Port:
- Server 5 Name: Server 5 Port:

At the bottom of the window, there are 'Submit' and 'Cancel' buttons. A small note at the bottom left reads: '* To use RADIUS for Request Authentication, please go to the Authentication Scheme Settings page.'

- Step 4** Check the **Enable RADIUS Servers** check box to enable RADIUS authentication.
- Step 5** In the Time to wait field, specify how long the Content Engine should wait before timing out. The default value is 5 seconds.
- Step 6** In the Number of Retransmits field, specify the number of attempts allowed to connect to a RADIUS server.
- Step 7** Check the **Enable Redirect** check box to enable RADIUS redirection.
- Step 8** Enter a redirect message for the user in the Redirect Message field. Three redirect messages are allowed.
- Step 9** In the Location field, enter a location where the redirect message should be sent. Three separate locations are allowed.
- Step 10** In the Shared Encryption Key field, enter the secret key that is used to communicate with the RADIUS server.
- Step 11** Enter an IP address or host name information in the Server Name field. Five different hosts are allowed.
- Step 12** In the Server Port field, enter the port number on which the RADIUS server is listening. Five different ports are allowed.
- Step 13** Click **Submit** to save the settings.

Table 13-3 RADIUS Server Settings

GUI Parameter	Function	CLI Command
Enable RADIUS Servers	Enables HTTP authentication using RADIUS servers.	radius-server enable
Time to wait	Number of seconds to wait for a response before timing out on a connection to a particular RADIUS server. The range is from 1 to 20 seconds. The default value is 5 seconds.	radius-server timeout
Number of retransmits	Number of attempts allowed to connect to a RADIUS server. The default value is 2 times.	radius-server retransmit
Enable redirect	Redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.	radius-server redirect enable
Redirect Message	Message sent to the user if redirection occurs.	radius-server redirect message
Location	Sets an HTML page location. This is the URL destination of the redirect message that is sent when authentication fails.	radius-server redirect message reply location url
Shared Encryption Key	Encryption key shared with the RADIUS server.	radius-server key keyword
Server Name	IP address or host name of the RADIUS server.	radius-server host {hostname ipaddress}
Server Port	Port number on which the RADIUS server is listening.	radius-server host auth-port port

Configuring TACACS+ Server Settings

The TACACS+ database validates users before they gain access to a Content Engine. TACACS+ is derived from the United States Department of Defense (RFC 1492) and is used by Cisco Systems as an additional control of nonprivileged and privileged mode access. ACNS 5.x software supports TACACS+ only and not TACACS or Extended TACACS.

To enable TACACS+ for HTTP request authentication, use the **tacacs enable** global configuration command.



Tip

The Content Distribution Manager does not cache user authentication information. Therefore, the user is reauthenticated against the TACACS+ server for every request. To prevent performance degradation caused by many authentication requests, install the Content Distribution Manager in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure TACACS+ server settings using the Content Distribution Manager GUI, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the name of the Content Engine that you want to configure. The Contents pane appears on the left.
- Step 3** From the Contents pane, choose **General Settings > Authentication > TACACS+ Server**. The TACACS+ Server Settings window appears. (See Figure 13-5.) Table 13-4 describes the fields in this window.

Figure 13-5 TACACS+ Server Settings Window

The screenshot shows the Cisco Application and Content Networking System GUI. The main window is titled "TACACS+ Server Settings for Content Engine, CONTENTENGINE". The left sidebar shows a tree view with "Contents" expanded, and "TACACS+ Server" selected. The main content area shows the following settings:

TACACS+ Server Settings	
Current applied settings from Content Engine, CONTENTENGINE	
Enable TACACS+ Servers *	<input checked="" type="checkbox"/>
Use ASCII Password Authentication:	<input type="checkbox"/>
Time to wait: *	<input type="text" value="0"/>
Number of retransmits: *	<input type="text" value="0"/>
Security Word:	<input type="text" value="***"/>
Primary Server: *	<input type="text" value="172.9.26.12"/>
Secondary Server:	<input type="text"/>
Tertiary Server:	<input type="text"/>

Below the settings, there are two notes:

- * To use TACACS+ for Request Authentication, please go to the Authentication Scheme Settings page.
- * To use TACACS+ for Login or Configuration Authentication, please go to the Login Authentication page.

A note at the bottom states: "Note: * - Required Field". At the bottom right, there are "Submit" and "Cancel" buttons.

- Step 4** Check the **Enable TACACS+ Servers** check box to enable TACACS+ authentication.
- Step 5** Check the **Use ASCII Password Authentication** check box to use the ASCII password type for authentication. The default password type is PAP (Password Authentication Protocol). However, you can change the password type to ASCII when the authentication packets are to be sent in ASCII clear text format.
- Step 6** In the Time to wait field, specify how long the Content Engine should wait before timing out. The default value is 5 seconds.
- Step 7** In the Number of Retransmits field, specify the number of attempts allowed to connect to a TACACS+ server. The default value is 2.
- Step 8** In the Security Word field, enter the secret key that is used to communicate with the TACACS+ server.
- Step 9** In the Primary Server field, enter an IP address or host name information for the primary TACACS+ server.

- Step 10** In the Secondary Server field, enter an IP address or host name information for a secondary TACACS+ server.
- Step 11** In the Tertiary Server field, enter an IP address or host name information for a tertiary TACACS+ server.
- Step 12** Click **Submit** to save the settings.

Table 13-4 TACACS+ Server Key Parameter Settings

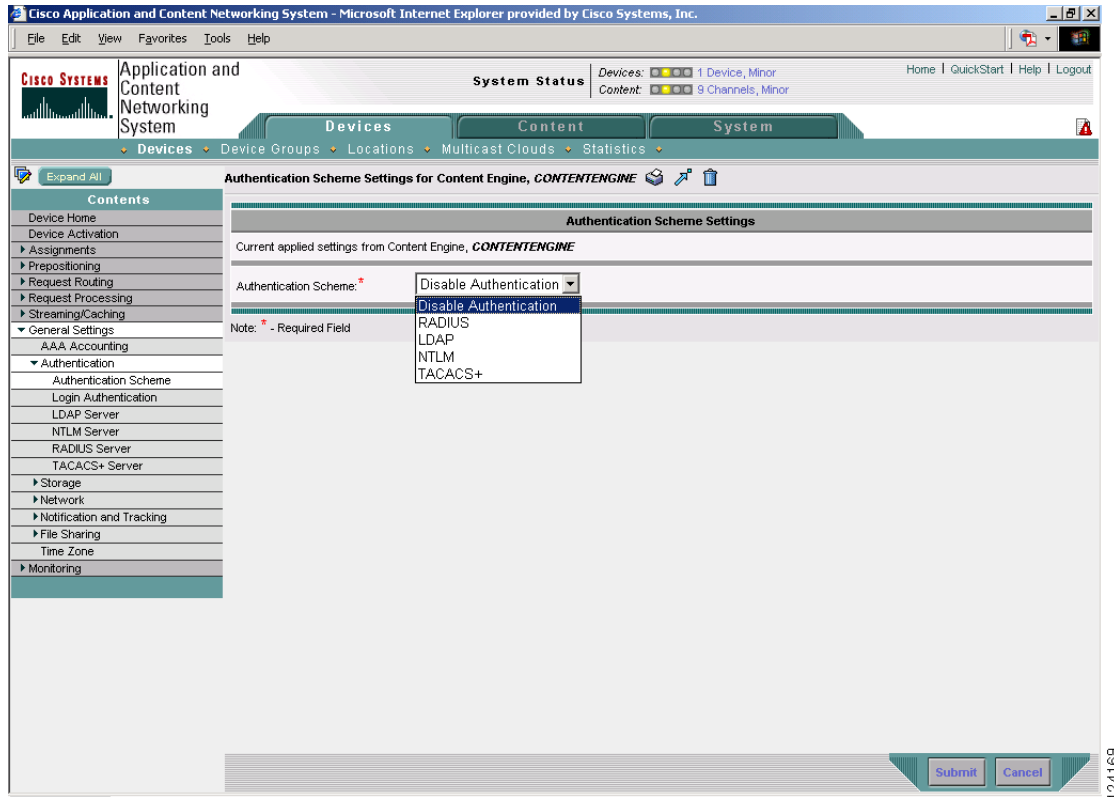
Key Parameter	Description	CLI Command
Enable TACACS+ Servers	Enables TACACS+ authentication.	tacacs enable
Use ASCII Password Authentication	Changes the default password type from PAP (Password Authentication Protocol) to ASCII clear text format.	tacacs password ascii
Time to wait	Number of seconds to wait for a response before timing out on a connection to a particular TACACS+ server. The range is from 1 to 20 seconds. The default value is 5 seconds.	tacacs timeout
Number of retransmits	Number of attempts allowed to connect to a TACACS+ server. The default value is 2 times.	tacacs retransmit
Security Word	Encryption key shared with the TACACS+ server.	tacacs key
Primary Server	IP address or host name of the primary TACACS+ server.	tacacs host {hostname ipaddress} [primary]
Secondary Server Tertiary Server	IP address or host name of the backup TACACS+ server. Up to 2 backup servers are allowed.	tacacs host {hostname ipaddress}

Setting the Authentication Scheme for Request Authentication

To enable an authentication scheme for request authentication, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the name of the Content Engine that you want to configure. The Contents pane appears on the left.
- Step 3** From the Contents pane, choose **General Settings > Authentication > Authentication Scheme**. (See [Figure 13-6](#).)

Figure 13-6 Authentication Scheme Settings Window



- Step 4** Choose an authentication scheme from the Authentication Scheme drop-down list.



Note You must configure and enable an authentication server before you can save the authentication scheme settings from this window.

- Step 5** Click **Submit** to save the settings.

Authentication Cache Size Adjustments

If the authentication cache is not large enough to accommodate all authenticated users at the same time, the Content Engine purges older entries that have not yet timed out. The Content Engine has a timeout value range from 1 to 1440 minutes (24 hours). Its default timeout value is 480 minutes.

The default time interval between the user's last Internet access and the removal of that user's entry from the authorization cache is 480 minutes. The minimum time interval is 1 minute, and the maximum is 24 hours. The Content Engine forces reauthentication with the access control server once this time interval expires.

When LDAP, RADIUS, and TACACS+ are used in proxy redirection mode, the authentication record kept in the authentication cache is indexed by the username and the password entered. When LDAP, RADIUS, and TACACS+ are used in WCCP-enabled router redirection mode, the authentication record indexed is the IP address of the Content Engine sending the request in transparent mode.

When an NTLM server is used in either proxy redirection mode or WCCP-enabled router redirection mode, all authentication records are indexed by using the IP address of the requesting Content Engine.

