CHAPTER 12

Configuring Login Authentication, Configuration Authorization, and Accounting

This chapter explains how to configure login (user) authentication and configuration authorization support for Content Distribution Managers, Content Engines, and Content Routers deployed in a centrally managed environment. It describes how to configure devices to use local authentication, RADIUS, or TACACS+ login authentication methods.

This chapter contains the following sections:

Note Login (user) authentication and authorization is independent of request authentication and authorization. For information about request authentication and authorization, see Chapter 15, "Configuring Request Authentication and Authorization."

Understanding Authentication, Authorization, and Accounting

Authentication determines who the user is and whether that user should be allowed access to the network or a particular device. It allows network administrators to bar intruders from their networks. It may use a simple database of users and passwords. It can also use one-time passwords.

Authorization determines what the user is allowed to do. It allows network managers to limit which network services are available to different users.

Accounting tracks what users did and when they did it. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

Collectively, authentication, authorization, and accounting are sometimes referred to as AAA. Central management of AAA means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

Understanding Login Authentication and Authorization

In the ACNS network, login authentication and authorization are used to control user access and configuration rights to Content Distribution Managers, Content Engines, and Content Routers. Login authentication is the process by which ACNS devices verify whether the person who is attempting to login to the device has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration privileges. The user account information is stored in an authentication, authorization, and accounting (AAA) database, and ACNS devices must be configured to access the particular authentication server (or servers) where the AAA database is lodged. When the user attempts to login to a device, the device compares the person's username, password, and privilege level to the user account information that is stored in the database.

Understanding User Accounts and Privilege Profiles

In a centrally managed ACNS network, user accounts can be created for access to the Content Distribution Manager and, independently, for access to the Content Engines and Content Routers that are registered to the Content Distribution Manager.

A privilege profile must be assigned to each new user account. ACNS software uses privilege profiles to determine which tasks a user can perform and the level of access provided.

There are two types of predefined privilege profiles:

- Normal user—User has read access and can see some of the Content Engine, Content Router, or Content Distribution Manager settings.
- Superuser—User has administrative privileges such as creating new users and modifying the Content Engine, Content Router, or Content Distribution Manager settings.

Users with administrative privileges can add, delete, or modify user accounts through the Content Distribution Manager GUI or the device CLI. For example, if an administrator logs in to a Content Engine with the predefined ACNS software superuser account (root administrator), the Content Engine grants that user the highest privilege level (level 15), which allows that user to perform any Content Engine administrative task during that login session.

For instance, that user could perform any of the following administrative tasks:

- Configure the Content Engine.
- Obtain statistical information that the Content Engine has collected.
- Reload the device.

Accessing a Device for the First Time

A Content Distribution Manager, Content Engine, or Content Router that is running ACNS software comes with a predefined superuser account that can be used initially to access the device and add other users.

When the system administrator logs in to a device before authentication and authorization have been configured, the administrator can access the device by using the default user account and password. Devices that are using ACNS software come with a single, predefined superuser user account (root administrator) that can be used for initial access to the device to initially configure the device and then add other user accounts. The username for this predefined superuser user account is *admin* and the default password is *default*. (If these defaults have been changed by another ACNS system administrator, you need to obtain the new username and password.)

Understanding AAA Database Management

User authentication data and user configuration privilege data can be maintained in any combination of these three databases in a centrally-managed ACNS network:

- Content Distribution Manager (local database)
- RADIUS server (external database)
- TACACS+ server (external database)

During Content Distribution Manager setup, you can choose to use an external access server or the internal (local) Content Distribution Manager-based authentication, authorization, and accounting (AAA) system for user access management. You can choose one method or any combination of the three methods.

If all three databases are enabled, then all databases are queried; if the user data cannot be found in the first database queried, then the second and third databases are queried. By default, Content Distribution Managers, Content Engines, and Content Routers use the local database to process login requests, with TACACS+ and RADIUS both disabled for login and configuration.

When the administrator logs in to a Content Distribution Manager, Content Engine, or Content Router, the device checks the specified authentication database to verify the user's username and password and to determine the access rights that this particular user should be granted during this login session.

Note In TACACS+ there is an "enable password" feature that allows an administrator to define a different enable password for each user. If an ACNS user logs in to the Content Engine with a normal user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), the user must enter the admin password to access privileged-level EXEC mode. This caveat applies even if these ACNS users are using TACACS+ for login authentication.

Default Login Authentication and Authorization Configuration

Table 12-1 lists the default configuration for login authentication and authorization.

Table 12-1 Default Configuration for Login Authentication and Authorization

Feature	Default Value
Login authentication	Enabled
Configuration authorization	Enabled
Authentication server failover because the authentication server is unreachable	Disabled
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ authorization (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ server timeout	5 seconds
TACACS+ retransmit attempts	2 times
RADIUS login authentication (console and Telnet)	Disabled
RADIUS authorization (console and Telnet)	Disabled
RADIUS server IP address	None specified

Table 12-1 Default Configuration for Login Authentication and Authorization (continued)

Feature	Default Value
RADIUS server UDP authorization port	Port 1645
RADIUS key	None specified
RADIUS server timeout	5 seconds
RADIUS retransmit attempts	2 times

You can change these defaults through the Content Distribution Manager GUI or through the device CLI, as described in the "Configuring Devices for Login Authentication and Authorization" section on page 12-7.

Understanding Login Authentication Failover

By default, ACNS devices fail over to the secondary method of login authentication whenever the primary login authentication method fails. In ACNS software Release 5.0.5 and later, you can change this default login authentication failover method. For centrally managed deployments, you can use the Content Distribution Manager GUI (for example, choose **Devices > Devices > General Settings > Authentication > Login Authentication** and check the **Enable Failover Server Unreachable** box) or the CLI (use the **authentication fail-over server unreachable** global configuration command) to enable the failover due to unreachable server option.

Failover occurs only if the specified authentication server is unreachable. The following example sets login authentication failover to occur if the authentication server is unreachable. In this case, the Content Engine will query the next authentication method only if the login authentication server is unreachable.

```
ContentEngine(config)#authentication fail-over server-unreachable
ContentEngine(config)#
```

To use the login authentication failover feature, you must set TACACS+, or RADIUS as the primary login authentication method, and local as the secondary login authentication method.

If the failover due to unreachable server option is enabled, then note the following:

- Only two login authentication schemes (a primary and secondary scheme) are allowed on the device.
- The device will fail over from the primary authentication scheme to the secondary authentication scheme only if all specified authentication servers of the primary authentication scheme are unreachable.

For example, if the failover due to server unreachable option is enabled and RADUIS is set as the primary login authentication scheme and local is set as secondary login authentication scheme, the following occurs:

1. When the device receives a login request, it queries all configured RADIUS authentication servers.
2. If one of the configured RADIUS servers is reachable, the device uses this RADIUS database to authenticate the user.
3. If all configured RADIUS servers are not reachable, the device tries the secondary authentication scheme (that is, it queries its local authentication database) to authenticate the user.

Note The local database will be contacted for authentication only if this RADIUS server is not reachable. In any other case (for example, if the authentication fails in the RADIUS server), then the local database is not contacted for authentication.

Conversely, if the failover due to unreachable server option is disabled, then the device contacts the secondary authentication database, regardless of the reason that the authentication failed with the primary authentication database.

If all the authentication databases are enabled for use, then all the databases are queried in the order of priority selected and based on the failover reason. If no failover reason is specified, then all databases are queried in the order of their priority. For example, first the primary authentication database is queried, then the secondary authentication database is queried, and finally the tertiary database is queried.

The local and the remote databases (TACACS+ and RADIUS) can be enabled or disabled through the Content Distribution Manager GUI or through the device CLI. The device verifies whether or not all are disabled and if so, sets the system to the default state (that is, local database is queried for authentication). (For information about this default state, see the "Default Login Authentication and Authorization Configuration" section on page 12-3.)

For more information on the various types of login authentication and authorization schemes, see the following sections:

- Understanding Local Login Authentication and Authorization, page 12-5
- Understanding RADIUS Authentication and Authorization, page 12-6
- Understanding TACACS+ Authentication and Authorization, page 12-6

For information about how to configure login authentication and authorization on Content Distribution Managers, Content Engines, and Content Routers, see the "Configuring Devices for Login Authentication and Authorization" section on page 12-7 and the

Understanding Local Login Authentication and Authorization

ACNS 5.x software provides authentication, authorization, and accounting (AAA) support for users who need a local access database with AAA features. Local login authentication can be configured on individual Content Engines using the Content Engine GUI or CLI, or when devices are managed centrally, local login can be configured using the Content Distribution Manager GUI.

When the primary login server and primary configuration server are set to local, usernames and passwords are local to each device and are not mapped to individual usernames. Local authentication and authorization uses locally configured login and passwords to authenticate login attempts.

By default, local login authentication is enabled first. You can disable local login authentication only after enabling one or more of the other login authentication methods. However, when local login authentication is disabled, if you disable all other login authentication methods, local login authentication is reenabled automatically.

Understanding RADIUS Authentication and Authorization

RADIUS is a client/server authentication and authorization access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response it receives from one or more RADIUS servers. RADIUS uses the User Datagram Protocol (UDP) for transport between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

Note For more information about how the RADIUS protocol operates, refer to RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can also specify which method to use first. For more information about configuring RADIUS authentication, see the "Configuring Devices for Login Authentication and Authorization" section on page 12-7.

Understanding TACACS+ Authentication and Authorization

TACACS+ controls access to network devices by exchanging Network Access Server (NAS) information between a network device and a centralized database to determine the identity of a user or an entity. TACACS+ is an enhanced version of TACACS, a User Datagram Protocol (UDP)-based access-control protocol specified by RFC 1492. TACACS+ uses TCP to ensure reliable delivery and encrypt all traffic between the TACACS+ server and the TACACS+ daemon on a network device.

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication. TACACS+ login authentication occurs when a user first logs on to the locally deployed Content Engine.

When a user requests restricted services, TACACS+ encrypts the user password information using the MD5 encryption algorithm and adds a TACACS+ packet header. This header information identifies the packet type being sent (for example, an authentication packet), the packet sequence number, the encryption type used, and the total packet length. The TACACS+ protocol then forwards the packet to the TACACS+ server.

A TACACS+ server can provide authentication, authorization, and accounting functions. These services, while all part of TACACS+, are independent of one another, so a given TACACS+ configuration can use any or all of the three services.

When the TACACS+ server receives a packet, it does the following:

- Authenticates the user information and notifies the client that login authentication has either succeeded or failed.
- Notifies the client that authentication will continue and that the client must provide additional information. This challenge-response process can continue through multiple iterations until login authentication either succeeds or fails.

You can configure a TACACS+ key on the client and server. If you configure a key on the Content Engine, it must be the same as the one configured on the TACACS+ servers. The TACACS+ clients and servers use the key to encrypt all TACACS+ packets transmitted. If you do not configure a TACACS+ key, packets are not encrypted.

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time. For more information about configuring TACACS+ as a login authentication scheme, see the next section.

Configuring Devices for Login Authentication and Authorization

To configure login authentication and authorization for a Content Distribution Manager, Content Engine or Content Router, complete the following tasks:

1. Determine the login authentication scheme that you want to configure the device to use when authenticating login requests. (For example, use the local database as the primary login database and your RADIUS server as the secondary authentication database.)
2. Configure the remote authentication server settings on the device (if a remote authentication database is to be used). (See the "Configuring Remote Authentication Server Settings for the Device" section on page 12-7.)

   For example, specify the IP address of the remote RADIUS servers or TACACS+ servers that the device should use to authenticate log-in requests.
3. Specify which authentication databases the device should check to process a login request. (See the "Configuring Login Authentication and Configuration Authorization Schemes for the Device" section on page 12-12.)
   - Specify the login authentication server failover scheme.
   - Specify the login server scheme.
   - Specify the config server scheme.

Caution Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

When local authentication is disabled, if you disable all other authentication methods, local authentication is reenabled automatically.

Configuring Remote Authentication Server Settings for the Device

If you have determined that your login authentication scheme is to include one or both external authentication servers, you must configure these server settings before you can configure the authentication scheme in the Content Distribution Manager GUI. The following sections provide steps for configuring RADIUS and TACACS+ server settings using the Content Distribution Manager GUI.

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 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.

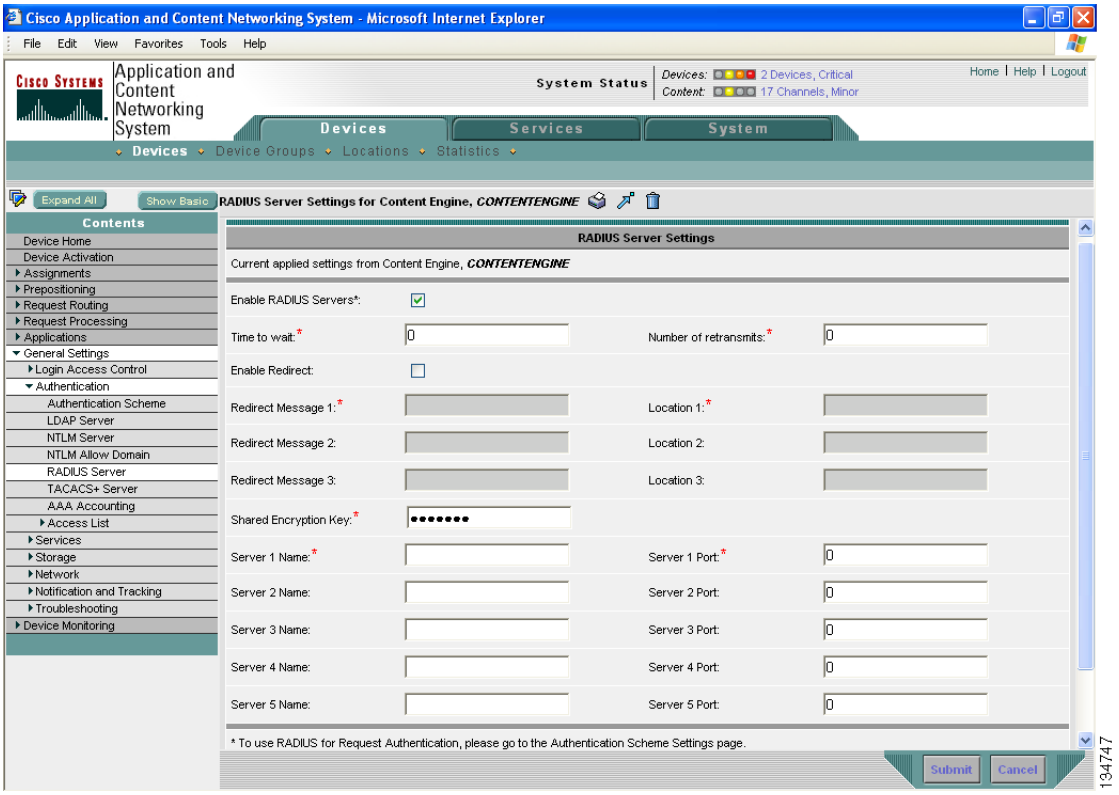
To configure RADIUS server settings using the Content Distribution Manager GUI, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the name of the device 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 12-1.) Table 12-2 describes the fields in this window.

Figure 12-1 RADIUS Server Settings Window



Step 4 To enable RADIUS authentication, check the **Enable RADIUS Servers** check box.

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 To enable RADIUS redirection, check the **Enable Redirect** check box.

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 a UDP port number on which the RADIUS server is listening. You must specify at least one port. Five different ports are allowed.

Step 13 To save the settings, click **Submit**.

Table 12-2 RADIUS Server Settings

Key Parameter	Description	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* or *ip-address*
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.

Tip The Content Distribution Manager does not cache user authentication information, so 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.

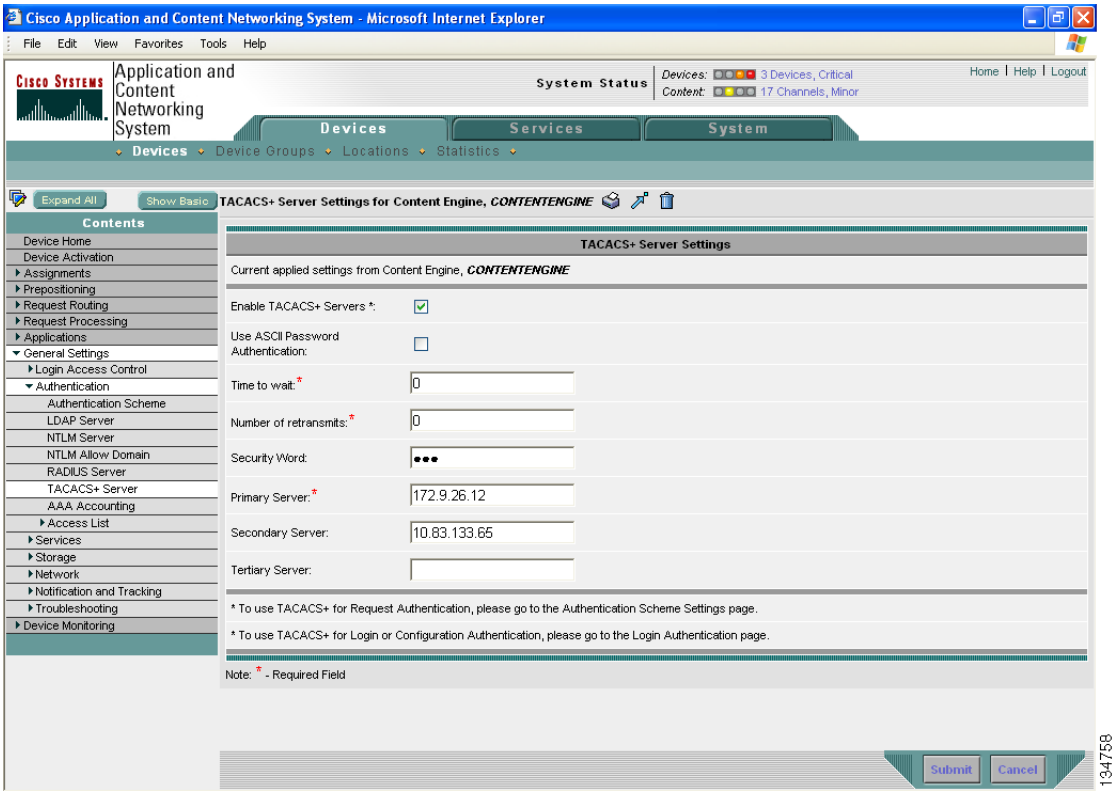
To configure TACACS+ server settings using the Content Distribution Manager GUI, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the name of the device 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 12-2.) Table 12-3 describes the fields in this window.

Figure 12-2 TACACS+ Server Settings Window



Step 4 To enable TACACS+ authentication, check the **Enable TACACS+ Servers** check box.

Step 5 To use the ASCII password type for authentication, check the **Use ASCII Password Authentication** check box. 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 To save the settings, click **Submit**.

Table 12-3 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 times that a connection to a TACACS+ server is allowed to be attempted before a connection is made. The default value is 2 times. The range is 1 to 3 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** *ip-address* or *hostname* [**primary**]
Secondary Server Tertiary Server	IP address or host name of the backup TACACS+ server. 2 backup servers are allowed.	**tacacs host** *ip-address* or *hostname*

Configuring Login Authentication and Configuration Authorization Schemes for the Device

To configure the login authentication and configuration authorization schemes for the device, follow these steps. In the following example, local is configured as the primary database, TACACS+ as the secondary database, and RADIUS as the tertiary database.

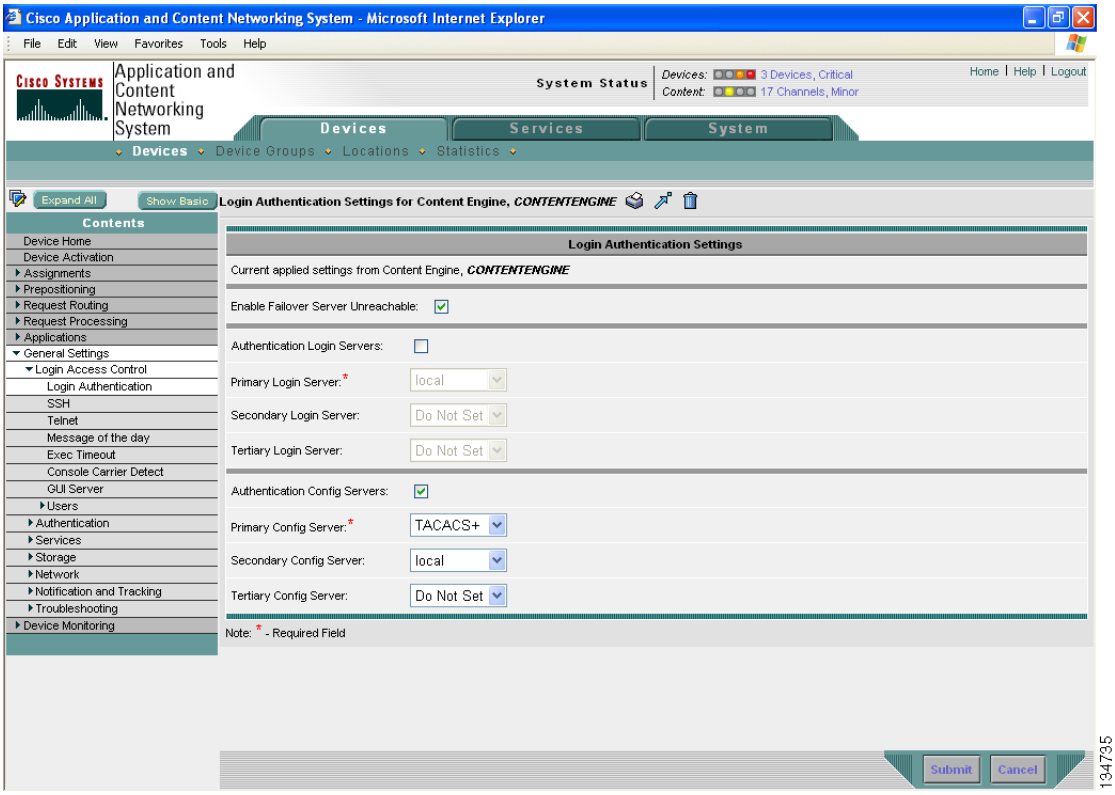
Note You must configure TACACS+ and RADIUS server settings for the device before you configure and submit these settings. See the "Configuring TACACS+ Server Settings" section on page 12-9 and the "Configuring RADIUS Server Settings" section on page 12-7 for information on how to configure these servers.

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the name of the device that you want to configure. The Contents pane appears on the left.

Step 3 From the Contents pane, choose **General Settings > Login Access Control > Login Authentication**. The Login Authentication Settings window appears. (See Figure 12-3.)

Figure 12-3 Login Authentication Settings Window



Step 4 To query the secondary authentication database if the primary authentication server is unreachable, check the **Enable Failover Server Unreachable** check box.

To use this feature, you must set TACACS+ or RADIUS as the primary authentication method and local as the secondary authentication method.

Step 5 To enable authentication privileges using the local, TACACS+, or RADIUS databases, check the **Authentication Login Servers** check box.

Step 6 From the Primary Login Server drop-down list, choose **local**.

Step 7 From the Secondary Login Server drop-down list, choose **TACACS+**.

Step 8 From the Tertiary Login Server drop-down list, choose **RADIUS**.

Step 9 To enable authorization privileges using the local, TACACS+, or RADIUS databases, check the **Authentication Config Servers** check box.

Step 10 From the Primary Config Server drop-down list, choose **local**.

Step 11 From the Secondary Config Server drop-down list, choose **TACACS+**.

Step 12 From the Tertiary Config Server drop-down list, choose **RADIUS**.

Step 13 To add authentication and authorization settings for the Content Engine, click **Submit**.

Changing the Admin Account Password for a Device

The default user account, *admin,* comes with the ACNS software and is preassigned the password *default*. This account allows access to all services and entities in the system. Cisco ACNS software allows any user with a role that gives them access to the Admin Password Setting window in the Content Distribution Manager GUI to configure a new password for the *admin* user account on individual Content Engines and Content Routers.

Note Each Content Engine or Content Router must have only one user account with the username *admin*. Therefore, the admin account password configuration is done per device, rather than at the system level.

To configure the admin password for a Content Engine or Content Router, follow these steps:

Step 1 From the Content Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**). The Devices (or Device Group) window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure the admin account password.

Step 3 In the Contents pane, choose **General Settings > Login Access Control > Users > Admin Password**. The Admin Password Setting window appears.

Step 4 In the Password field, enter a password.

Step 5 In the Confirm Password field, reenter the password.

Step 6 Click **Submit** to save the new password.

Configuring User Accounts for Centrally Managed Devices

Cisco ACNS software allows you to create, modify, and delete user accounts for login access to individual devices (Content Engines and Content Routers) or device groups that are registered with a Content Distribution Manager.

Creating User Accounts for Centrally Managed Devices

To create a new user account from the Content Distribution Manager GUI, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to create new user account. The Device Home window for the chosen device appears.

Step 3 In the Contents pane, choose **General Settings > Login Access Control > Users > Usernames**. The Usernames window for the chosen device (or device group) appears.

The Aggregate Settings **Yes** radio button is selected by default, and usernames are displayed for the Content Engine, as well as for any associated device groups. The settings for the Usernames for device groups cannot be modified or deleted; they are read-only. However, you can modify the Usernames for the Content Engine. If you click the Aggregate Settings **No** radio button, you can view and modify the Usernames for the Content Engine only. The Usernames for any associated device groups are not displayed.

Step 4 Click the **Create New Username** icon from the taskbar. The Creating New Local User for the device window appears.

Step 5 In the Username field, enter the username.

Step 6 In the Password field, enter the password for the user account.

Step 7 In the Confirm Password field, retype the password.

Step 8 In the Cifs Password field, enter the Windows user password.

Step 9 In the Confirm Cifs Password field, retype the Windows user password.

Step 10 From the Privilege drop-down list, choose **Super User** to create a user account with admin privileges. Alternatively, to create a user account without admin privileges, choose **Normal User**.

Step 11 To save the settings, click **Submit**.

This GUI procedure corresponds to the following global configuration CLI command:

username *name* {**cifs-password | password | privilege**}

Modifying and Deleting User Accounts for Centrally Managed Devices

To modify an existing user account, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to modify the user account information.

Step 3 In the Contents pane, choose **General Settings > Login Access Control > Users > Usernames**. The Usernames window for the chosen device (or device group) appears.

Step 4 In the Username field, edit the name of the user, if needed.

Step 5 Edit other information or settings as needed.

Step 6 To save your settings, click **Submit**.

Note Deleting a user account from the CLI does *not* disable the corresponding user account in the CMS database. Consequently, the user account remains active in the CMS database. User accounts created in the Content Distribution Manager GUI should always be deleted from the Content Distribution Manager GUI.

To delete a user account from the Content Distribution Manager GUI, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to delete a user account.

Step 3 In the Contents pane, choose **General Settings > Login Access Control > Users > Usernames**. The Usernames window for the chosen device (or device group) appears.

Step 4 In the taskbar, click the **Trash** icon.

Step 5 To confirm the action, click **OK**.

Managing User Accounts and Privilege Profiles for the Content Distribution Manager

In a service provider environment, it is necessary to manage user authorization to services and access to domains (sets of Content Engines, device groups, and content providers). Typically, a service provider creates a user account for itself with administrator-level privileges, and then it creates user accounts for its customers. Service provider customers then have the ability to set up and manage user accounts on their own, which inherit the same level of rights as their main customer account unless the customers choose to limit user account privileges further.

ACNS 5.x software provides services for Content Distribution Manager user administration, role management, domain management, and accounting. These services can be configured in the Content Distribution Manager GUI.

Tasks include the following:

- Creating and Managing User Accounts for the Content Distribution Manager, page 12-16
- Creating and Managing Roles, page 12-20
- Configuring and Managing Domains, page 12-23
- Changing Your CLI User Password, page 12-20

ACNS 5.5 software supports a *user manager* account for creating and managing Content Distribution Manager user accounts. The user manager is responsible for creating a group of Content Distribution Manager user accounts, assigning roles and domains, as well as modifying any other user accounts in the Content Distribution Manager. User managers must be assigned the admin role, which authorizes all services and access to all domains. Only Content Distribution Manager users with administrator-level authorization are allowed to create and manage Content Distribution Manager user accounts.

After an upgrade to ACNS 5.5 software, any user accounts that do not meet the above requirement are prevented from performing user manager services. In other words, these users can log in to the Content Distribution Manager GUI but do not have access to the User Management pages (System > Users). These accounts can access the User Management pages by having their authorization increased to the administrator role. This can only be done by those Content Distribution Manager users with the administrator role.

Creating and Managing User Accounts for the Content Distribution Manager

Note This section is addressed to users with administrator-level privileges (admin users) only.

When you create a user account, you enter information about the user. A user account contains a username, the name of the individual who owns the account, contact information, job title, and department. All user account information is stored in an internal database on the Content Distribution Manager.

Each user account can then be assigned to a role and a domain. A *role* defines which Content Distribution Manager GUI configuration pages the user can access and which services the user has authority to configure or modify. A *domain* defines which entities in the network the user can access and configure or modify. You can assign a user account to zero or more roles, and to zero or more domains.

Two default user accounts are preconfigured in the Content Distribution Manager and come with the ACNS software. The first account, called *admin*, is assigned the administrator role that allows access to all services and access to all entities in the system. This account cannot be deleted from the system, but it can be modified. Only the username and the role for this account are unchangeable.

The second preconfigured user account is called *default*. Any user account that is authenticated but has not been registered in the Content Distribution Manager obtains the access rights (role and domains) assigned to the default account. This account is configurable, but it cannot be deleted nor its username changed.

Using the Content Manager Distribution GUI, you can perform these tasks:

- Create a new user account.
- Modify and delete existing user accounts.
- View all user accounts in the system.

Creating New User Accounts Using the Content Distribution Manager GUI

When you create a new user account in the Content Distribution Manager GUI, you have the option to create the user account in the CLI at the same time. Using this GUI option to create the new account in the CLI provides the following benefits:

- The user account is created in the primary Content Distribution Manager management database and in the CLI from one central point.
- The user account is also created in the standby Content Distribution Manager management database and in the CLI from one central point.
- Users can change their passwords, and the password change will propagate to standby Content Distribution Managers.

If you choose to create the user account from the GUI *without* creating the user account in the CLI at the same time from the GUI, the following results apply:

- The user account is created in the primary and standby Content Distribution Manager management databases.
- No user account is created in the CLI, and the user *cannot* log in to the Content Distribution Manager GUI until an account is created from the CLI.
- Local users cannot change their passwords using the GUI.
- Local users can change their passwords using the CLI; however, the password change is not propagated from the CLI to the CMS when the CLI user option is enabled in the GUI.

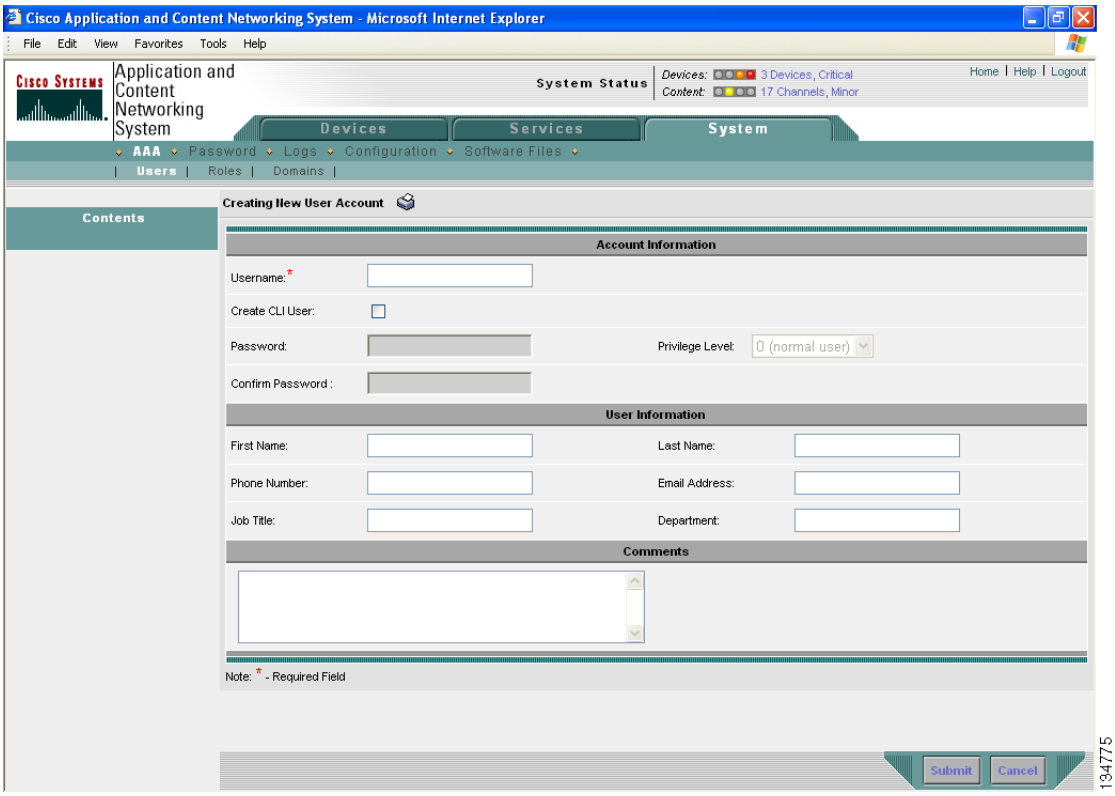
  If a user account has been created from the CLI only, when you log in to the Content Distribution Manager for the first time, the Centralized Management System (CMS) automatically creates a user account (with the same username as configured in the CLI) with default authorization and access control. However, to change the password in this scenario, the user account must be explicitly configured from the GUI with CLI user option enabled.

To create a new user account, follow these steps:

Step 1 Choose **System > AAA > Users**. Click the **Create New User Accounts** icon. The Creating New User Account window appears. (See Figure 12-4.)

Note This window can only be accessed by users with administrator-level privileges.

Figure 12-4 Creating New User Account Window



Step 2 In the Username field, enter the user account name.

Step 3 If you want to create a local user account with password and privilege level from the Content Distribution Manager GUI, click the **Create CLI User** check box. The user account is created automatically in the CLI. To deny creating a CLI user account from the GUI, leave the box unchecked.

Step 4 In the Password field, enter a password for the CLI user account, and reenter the same password in the Confirm Password field.

Step 5 From the drop-down list, choose a privilege level for the CLI user account. The choices are 0 (zero) (normal user) or 15 (superuser). The default value is 0.

Note A superuser can use privileged EXEC-level commands, whereas a normal user can use only user-level EXEC commands.

Step 6 In the Username fields, enter the following information about the user: First Name, Last Name, Phone Number, Email Address, Job Title, and Department.

Step 7 In the Comments field. enter any additional information about this account.

Step 8 To save your settings, click **Submit**.

Modifying and Deleting User Accounts

Note Modifying a user account from the CLI does not update the Centralized Management System (CMS) database.

To modify an existing user account, follow these steps:

Step 1 In the Content Distribution Manager GUI, choose **System > AAA > Users**. The User Accounts window appears.

Step 2 Click the **Edit** icon next to the user account that you want to modify. The Modifying User Account window appears.

Note This window can only be accessed by users with administrator-level privileges.

Step 3 In the Username field, edit the name of the user, if needed.

Step 4 To make the password fields and privilege level drop-down list available for modification, check the **Change CLI User Password**.

Step 5 Edit other information or settings as needed.

Step 6 To save your settings, click **Submit**.

Note Deleting a user account from the CLI does *not* disable the corresponding user account in the CMS database. Consequently, the user account remains active in the CMS database. User accounts created in the Content Distribution Manager GUI should always be deleted from the Content Distribution Manager GUI.

To delete a user account from the Content Distribution Manager GUI, follow these steps:

Step 1 In the Content Distribution Manager GUI, choose **System > AAA > Users**. The User Accounts window appears.

Step 2 Click the **Edit** icon next to the user account that you want to delete. The Modifying User Account window appears.

Note This window can only be accessed by users with administrator-level privileges.

Step 3 In the taskbar, click the **Trash** icon.

Note If the CLI user account was created using the GUI, the corresponding CLI user account is removed from the CLI and is also deleted from all standby Content Distribution Managers.

Step 4 To confirm the action, click **OK**.

Changing Your CLI User Password

If you are a user *without* admin privileges and you are logged in to the Content Distribution Manager GUI, you can change your own CLI user password if you meet the following requirements:

- Your CLI user account and password were created in the Content Distribution Manager GUI and not in the CLI.
- You are authorized to access the password window.

Note We do not recommend changing the CLI user password from the CLI. Any changes to CLI user passwords from the CLI are *not* updated in the management database and are not propagated to the standby Content Distribution Manager. Therefore, passwords in the management database will not match a new password configured in the CLI.

Note The advantage of initially setting passwords from the Content Distribution Manager GUI is that both the primary and the standby Content Distribution Managers will be synchronized, and GUI users will not have to access the CLI to change their password.

To change your CLI user password, follow these steps:

Step 1 In the Content Distribution Manager GUI, choose **System > Password**. The Changing Password for User Account window appears.

Step 2 In the New Password field, enter the changed password.

Step 3 in the Confirm New Password field, reenter the password for confirmation.

Step 4 To save your settings, click **Submit**.

Viewing User Accounts

To view all user accounts, choose **System > AAA> Users** from the Content Distribution Manager GUI. The User Accounts window displays all the user accounts in the management database.

Creating and Managing Roles

The Content Distribution Manager provides many types of services. Not all users have access to all services. Users are assigned a role, which indicates the services to which they have access. A *role* is a set of enabled services.

Each user account can be assigned to zero or more roles. Roles are not inherited or embedded. Using the Content Distribution Manager GUI, you can perform these tasks:

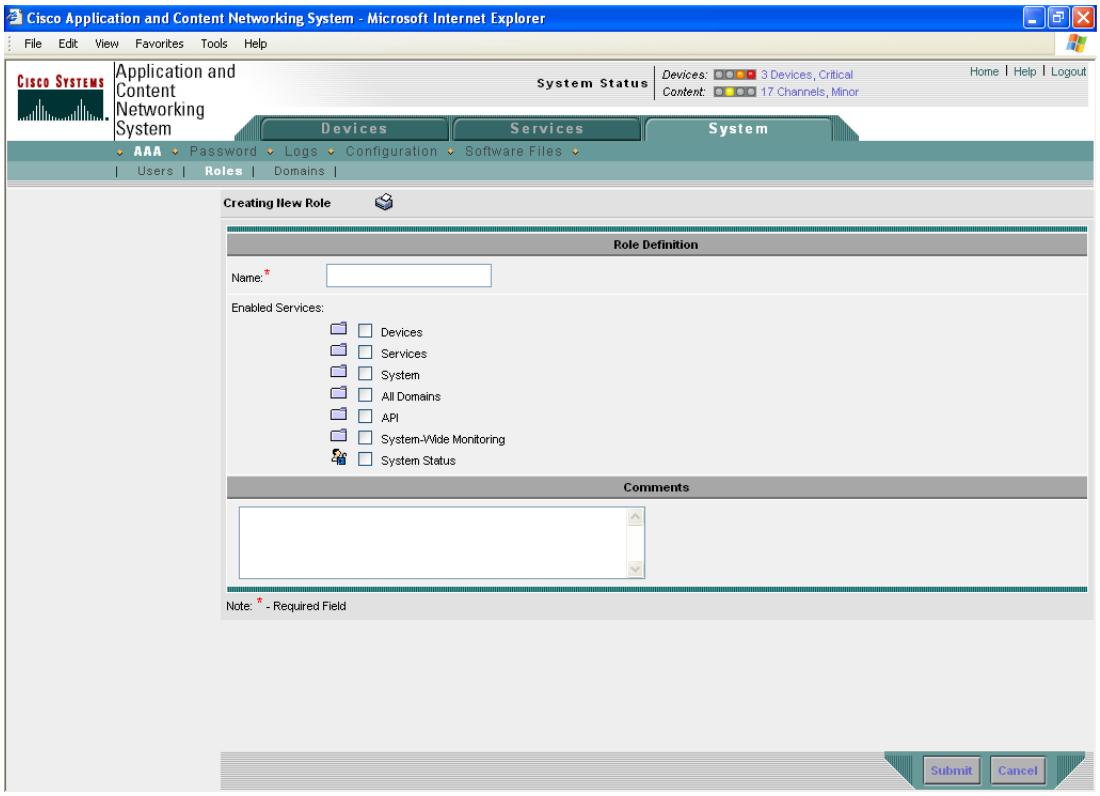
- Create new roles.
- Modify and delete existing roles.
- Assign roles to user accounts.
- View all roles in the system.

The Content Distribution Manager provides one predefined role, known as the admin role. The admin role has access to all services and all ACNS network entities. To create a role, follow these steps:

Step 1 Choose **System > AAA > Roles**. The Roles listing window appears.

Step 2 In the taskbar, click the **Create New Role** icon. The Creating New Role window appears. (See Figure 12-5.)

Figure 12-5 Creating New Role Window



Step 3 In the Name field, enter the name of the role.

Step 4 To expand the listing of services under that category, click a folder, and then check the check box next to the service or services that you want to enable for this role. To choose all the services under one category simultaneously, check the check box next to the top-level folder for those services.

Step 5 Enter any comments about this role in the Comments field.

Step 6 To save your settings, click **Submit**.

Modifying and Deleting Roles

Note The admin user account, by default, is allowed access to all services and cannot be modified.

To modify a role, follow these steps:

Step 1 Choose **System > AAA > Roles**. The Roles window appears.

Step 2 To modify an existing role, click the **Edit** icon next to the name of the role you want to change. The Modifying Role window appears.

Step 3 In the Name field, enter a new name or change the existing name of the role.

Step 4 To enable a service for this role, check the check box next to the services that you want. To disable a previously selected service, uncheck the check box next to the service you want to disable. To choose all the services under one category simultaneously, check the check box next to the top-level service.

Step 5 In the Comments field, enter any comments about this role.

Step 6 To save your settings, click **Submit**.

Viewing Role Settings

You might want to view role settings before assigning a role to a particular user account.

To view role settings, follow these steps:

Step 1 Choose **System > AAA > Users**. The User Accounts window appears with all configured user accounts listed.

Step 2 Click the **Edit** icon next to the user account for which you want to assign roles. The Modifying User Account window appears.

Step 3 In the Contents pane, choose **Role Management**. The Role Management for User Account User window appears.

Step 4 In the Role Management for User Account User window, click the **View** (eyeglass) icon next to the role name to display a new popup window called the Viewing Role window.

The role names, comments about this role, and services that are enabled for this role are displayed.

Step 5 After you have finished viewing the settings, click **Close**.

Assigning Roles to User Accounts

Note The admin user account, by default, is assigned to the role that allows access to all domains and all entities in the system. It is not possible to change the role for this user account.

To assign roles to user accounts, follow these steps:

Step 1 Choose **System > AAA > Users**. The User Accounts window appears with all configured user accounts listed.

Step 2 Click the **Edit** icon next to the user account for which you want to assign roles. The Modifying User Account window appears.

Step 3 In the Contents pane, choose **Role Management**. The Role Management for User Account User window appears with all configured role names listed.

Step 4 Click the **Assign** icon (blue cross mark) that appears next to the role name that you wish to assign to the selected user account.

Step 5 To unassign a previously assigned user account role, click the **Unassign** (green tick mark) next to the role name.

Note Click the **Assign all Roles** icon in the taskbar to assign all roles in the current window to a user account. Alternatively, click the **Remove all Roles** icon to unassign all roles associated with a user account.

Step 6 To save your settings, click **Submit**. A green tick mark appears next to the assigned roles and a blue cross mark appears next to the unassigned roles. The roles assigned to this user account will be listed in the Roles section in the Modifying User Account window.

Configuring and Managing Domains

A *domain* is a set of ACNS network entities or objects that make up the ACNS network. Whereas a role defines which services a user can perform in the ACNS network, a domain defines which entities the user has access to. The Content Distribution Manager GUI provides three predefined entities. An *entity* can be a Content Engine, content provider, or device group. These predefined entities are treated like services and can be enabled or disabled when you set up user roles.

When you configure a domain, you can choose to include Content Engines, content providers, or device groups in the domain. Using the Content Distribution Manager GUI, you can perform these tasks:

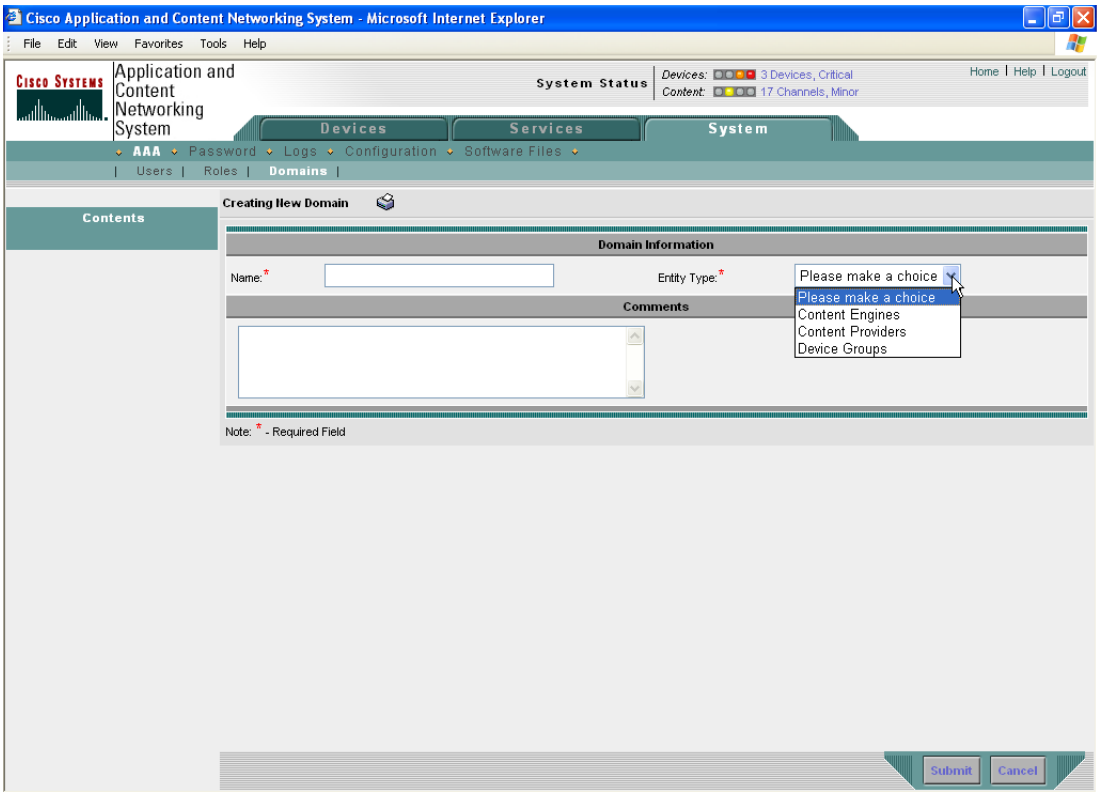
- Create new domains.
- Modify and delete existing domains.
- View all domains in the system.

To create a new domain, follow these steps:

Step 1 Choose **System > AAA > Domains**. The Domains listing window appears.

Step 2 In the taskbar, click the **Create New Domain** icon. The Creating New Domain window appears. (See Figure 12-6.)

Figure 12-6 Creating New Domain Window



Step 3 In the Name field, enter the name of the domain.

Step 4 From the Entity Type drop-down list, choose the entity type that you want to assign to the domain. Entity choices include Content Engines, content providers, or device groups.

Step 5 In the Comments field, enter any comments about this domain.

Step 6 To save your settings, click **Submit**. If the entity type you chose has not already been assigned to the domain, then a message indicating that the entity type has not been assigned appears.

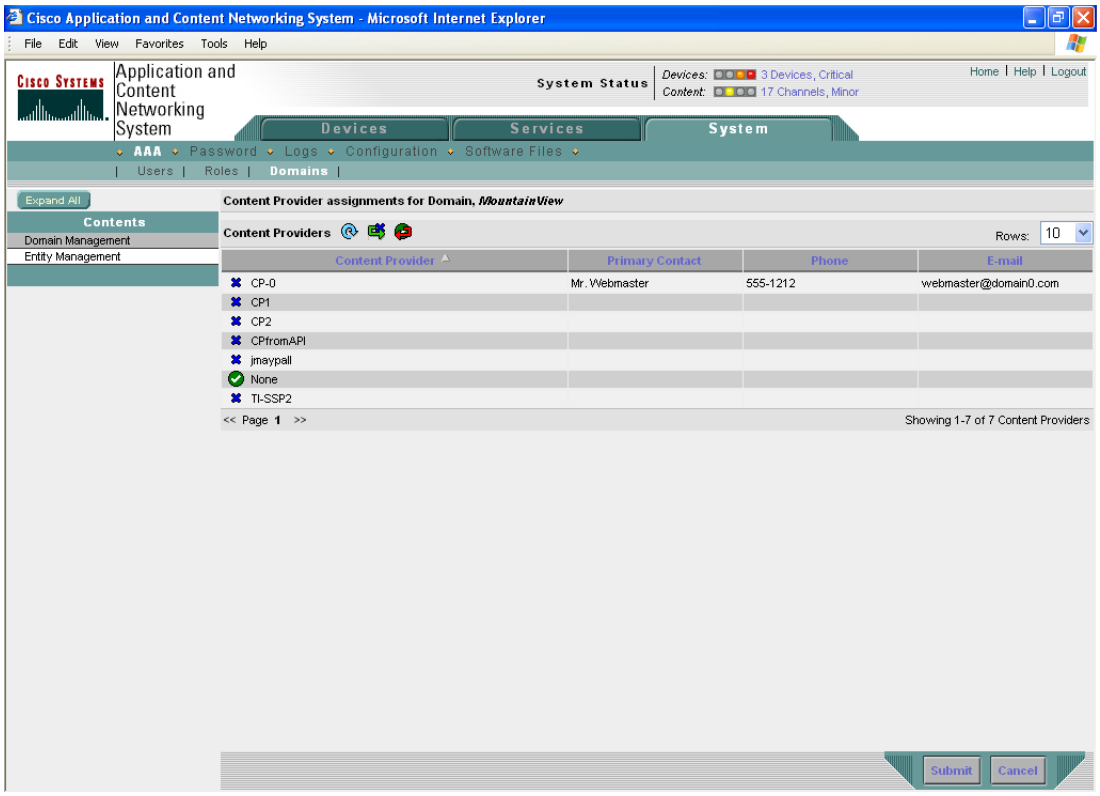
Adding an Entity to a Domain

To add an entity to a domain, follow these steps:

Step 1 Choose **System > AAA > Domains** and, click the **Edit** icon next to the name of the domain that you want to modify.

Step 2 In the Contents pane, choose **Entity Management**. The *Entity_name* Assignments for Domain window for the current domain appears. (See Figure 12-7.) In Figure 12-7, the entity is a content provider.

Figure 12-7 Entity Assignment to Domain Window—Content Provider Entity Shown



Step 3 To add an entity to the current domain, click the **Assign** icon (blue cross mark) next to the name of the entity that you want to add. A green tick mark appears next to the selected entity when you submit the settings.

Alternatively, to add all entities to the selected domain, click the **Assign all** icon in the taskbar.

Step 4 To remove an entity from the current domain, click the **Unassign** icon (green tick mark) next to the name of the entity that you want to remove from the domain. A blue cross mark appears next to the unassigned entity after you submit the settings.

Alternatively, to remove all entities from the domain, click the **Remove all** icon in the taskbar.

Step 5 To save your settings, click **Submit**.

Modifying and Deleting Domains

To modify or delete an existing domain, follow these steps:

Step 1 Choose **System > AAA > Domains**. The Domains window appears.

Step 2 Click the **Edit** icon next to the domain that you want to modify. The Modifying Domain window appears.

Step 3 Modify the settings as desired.

Step 4 To save your settings, click **Submit**.

Step 5 To delete the domain, click the **Trash** icon in the taskbar.

Step 6 To confirm the action, click **OK**.

Viewing Domains

To view the domain configuration for a particular user account, follow these steps:

Step 1 Choose **System > AAA > Users**. The User Accounts window appears with all configured user accounts listed.

Step 2 Click the **Edit** icon next to the user account for which you want to view the domain configuration. The Modifying User Account window appears.

Step 3 In the Contents pane, choose **Domain Management**. The Domain Management for User Account User window appears.

Step 4 To display a new popup window called the Viewing Domain window, click the **View** (eyeglass) icon next to the domain name.

The domain name, entity type, comments about this domain, and entities assigned to this domain are displayed.

Step 5 After you have finished viewing the settings, click **Close**.

Assigning Domains to User Accounts

To assign domains to user accounts, follow these steps:

Step 1 Choose **System > Users**. The User Accounts window appears with all configured user accounts listed.

Step 2 Click the **Edit** icon next to the user account for which you want to assign domains. The Modifying User Account window appears.

Step 3 In the Contents pane, choose **Domain Management**. The Domain Management for User Account User window appears with all configured domains and their entity types listed.

Step 4 Click the **Assign** icon (blue cross mark) that appears next to the domain name that you wish to assign to the selected user account.

Step 5 To dissociate an already associated domain from the user account, click the **Unassign** (green tick mark) next to the domain name.

Note To assign all domains in the current window to a user account, click the **Assign all Domains** icon in the taskbar. Alternatively, to unassign all domains associated with a user account, click the **Remove all Domains** icon.

Step 6 To save your settings, click **Submit**. A green tick mark appears next to the assigned domains, and a blue cross mark appears next to the unassigned domains. The domains assigned to a user account are listed in the Domains section in the Modifying User Account window.

Configuring AAA Accounting

Accounting tracks all user actions and when the actions occurred. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

The ACNS accounting feature uses TACACS+ server logging. Accounting information is sent to the TACACS+ server only, not to the console or any other device. The syslog file on the Content Engine logs accounting events locally. The format of events stored in the syslog is different from the format of accounting messages.

The TACACS+ protocol allows effective communication of AAA information between Content Engines and a central server. It uses TCP for reliable connections between clients and servers. Content Engines send authentication and authorization requests, as well as accounting information to the TACACS+ server.

Note Before you can configure the AAA accounting settings for any device, you must first configure a TACACS+ server for the device. (See the "Configuring TACACS+ Server Settings" section on page 12-9.)

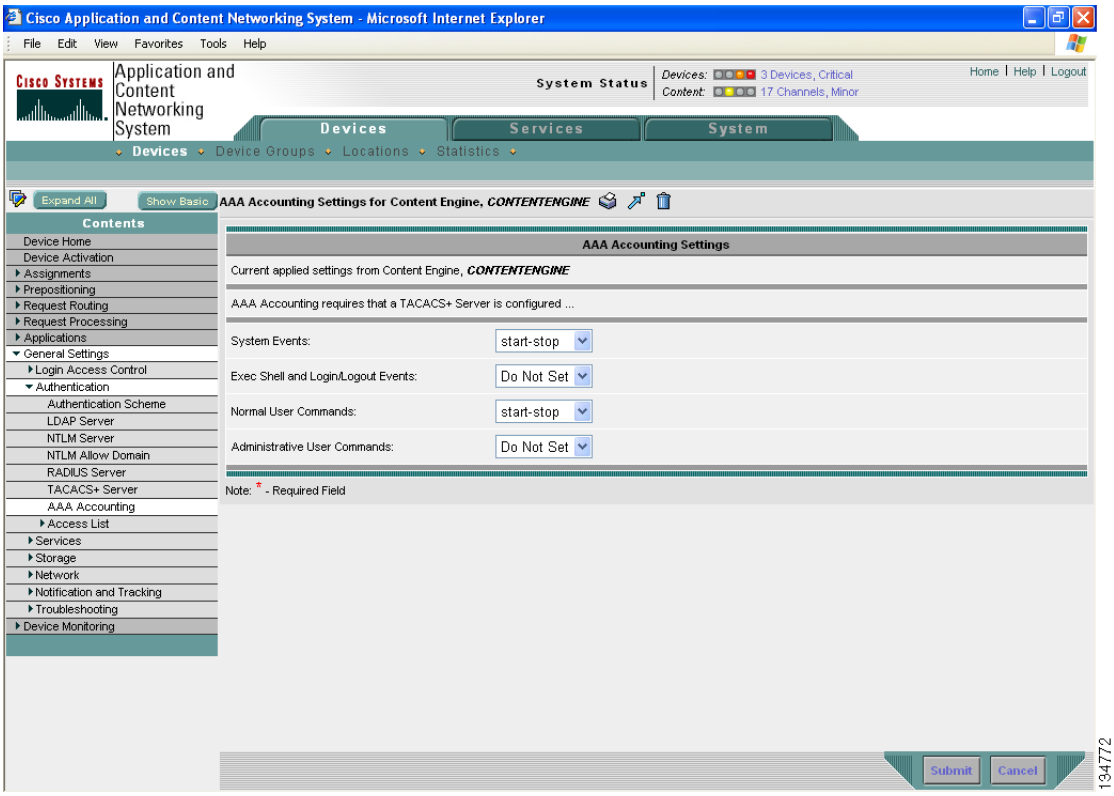
To configure AAA accounting settings, follow these steps:

Step 1 From the Content Distribution Manager GUI, choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the name of the device that you want to configure. The Device Home window appears.

Step 3 In the Contents pane, choose **General Settings > Authentication > AAA Accounting**. The AAA Accounting Settings window appears. (See Figure 12-8.) Table 12-4 describes the fields in this window and provides the corresponding CLI global configuration commands that are available on the Content Distribution Manager.

Figure 12-8 AAA Accounting Settings Window



Step 4 To activate accounting for system events, choose a keyword from the **System Events** drop-down list that indicates when accounting is to take place.

Step 5 To activate accounting for EXEC mode processes, choose a keyword from the **Exec Shell and Login/Logout Events** drop-down list that indicates when accounting is to take place.

Step 6 To activate accounting for all commands at the normal user level, choose a keyword from the **Normal User Commands** drop-down list that indicates when accounting is to take place.

Step 7 To activate accounting for all commands at the administrative user level, choose a keyword from the **Administrative User Commands** drop-down list that indicates when accounting is to take place.

Caution Before using the **wait-start** option, make sure that your Content Engine is configured with the TACACS+ server and is able to successfully contact the server. If the Content Engine cannot contact a configured TACACS+ server, it might become unresponsive.

Table 12-4 AAA Accounting Settings

GUI Parameter	Function	CLI Command
Event Type		
System Event	Accounting for all system-level events not associated with users, such as reloads.	**aaa accounting system default** {**start-stop** | **stop-only**} **tacacs**

Table 12-4 AAA Accounting Settings (continued)

GUI Parameter	Function	CLI Command
Exec Shell and Login/Logout Events	Accounting for EXEC shell and user login and logout events on the Content Engine. Reports include username, date, start and stop times, and Content Engine IP address.	**aaa accounting exec default** {**start-stop** | **stop-only** | **wait-start**} **tacacs**
Normal User Commands	Accounting for all commands at the normal user privilege level.	**aaa accounting commands 0 default** {**start-stop** | **stop-only** | **wait-start**} **tacacs**
Administrative User Commands	Accounting for all commands at the administrative user privilege level.	**aaa accounting commands 15 default** {**start-stop** | **stop-only** | **wait-start**} **tacacs**
Options		
stop-only	The Content Engine sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.	**aaa accounting** {**commands** | **exec** | **system**} **default stop-only tacacs**
start-stop	The Content Engine sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server. The start accounting record is sent in the background. The requested user service begins regardless of whether or not the start accounting record was acknowledged by the TACACS+ accounting server.	**aaa accounting** {**commands** | **exec** | **system**} **default start-stop tacacs**
wait-start	The Content Engine sends both a start and a stop accounting record to the TACACS+ accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.	**aaa accounting** {**commands** | **exec**} **default wait-start tacacs**
Do Not Set	Accounting is disabled for the specified event.	**no aaa accounting**

Step 8 To save the settings, click **Submit**.

Viewing Audit Trail Logs

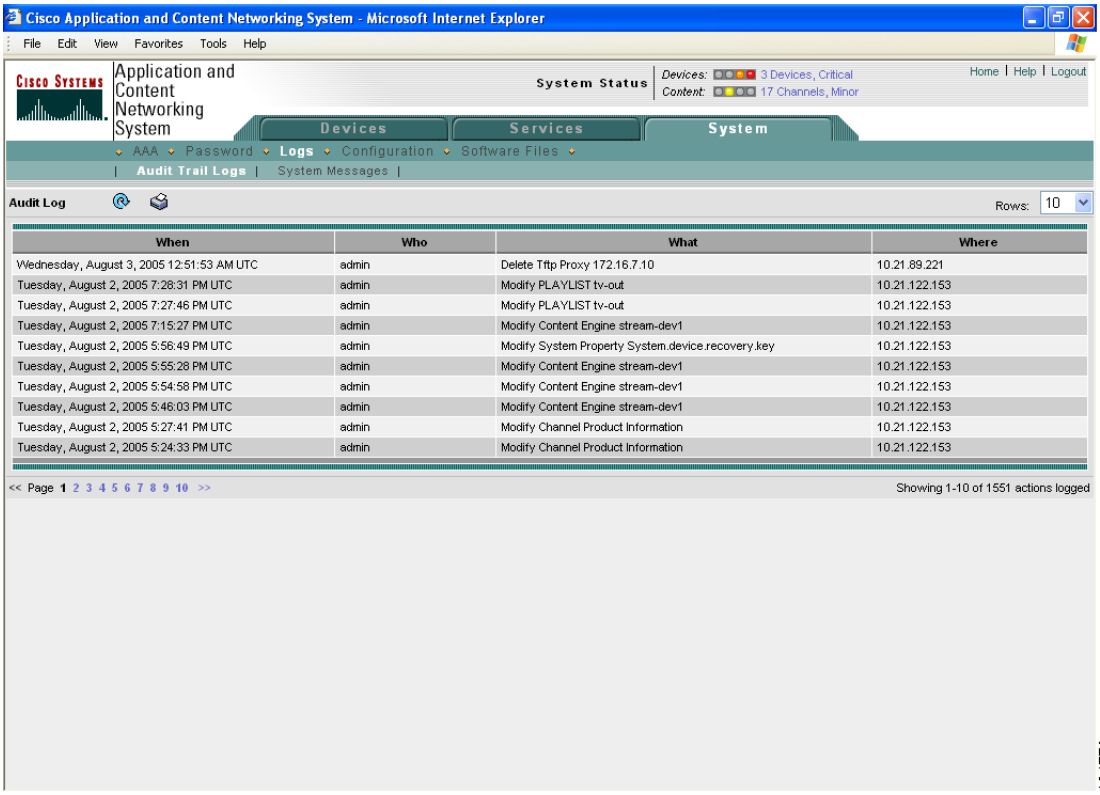
The Content Distribution Manager logs user activity in the system. The only activities that are logged are those that change the ACNS network. This feature provides accountability for users actions, for example, which user did what and when. Logged activities include the following:

- Creation of ACNS network entities
- Modification and deletion of ACNS network entities
- System configurations

To view audit trail logs, follow these steps:

Step 1 Choose **System > Logs > Audit Trail Logs**. The Audit Log window appears. (See Figure 12-9.) All logged transactions in the Content Distribution Manager are listed by date and time, user, actual transaction that was logged, and the IP address of the machine that was used.

Figure 12-9 Audit Log Window



Step 2 To determine the number of rows that you want to display, choose a number from the Rows drop-down list.