Creating and Managing Administrator User Accounts and Groups

This chapter describes how to create user accounts and groups from the WAAS Central Manager GUI.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances, WAE Network Modules (the NME-WAE family of devices), and SM-SRE modules running WAAS.

This chapter contains the following sections:

Overview of Administrator User Accounts

Your WAAS system comes with an administrator account already created that you can use to access the WAAS Central Manager GUI as well as the WAAS CLI. This account has a username of *admin* and a password of *default*. You can use the WAAS Central Manager GUI to change the password of this account.

If you want to create additional administrator user accounts, see Table 8-1 for a description of the two types of accounts you can create from the WAAS Central Manager GUI.

Table 8-1   ***Account Type Descriptions***

Account Type	Description
Roles-based account	Allows you to create accounts that manage and configure specific WAAS services. For example, you may want to delegate the configuration of application acceleration to a specific administrator. In this case, you could create a roles-based account that only has access to the Acceleration pages in the WAAS Central Manager GUI.
	You can also create a roles-based account that only has access to the WAE Device Manager instead of the WAAS Central Manager GUI. And you can create a role-based account that also is a local user account.
	You create roles-based accounts from the Admin menu in the WAAS Central Manager GUI.
Local account	Provides CLI access to WAE devices and optionally allows users to access the WAE Device Manager GUI. A user with this account type can log into the WAAS Central Manager but they have the access rights assigned to the default account, which initially has access to no GUI functionality.
	We recommend that you create a local account if there is an administrator that only needs CLI access to WAE devices or to the WAE Device Manager GUI.
	You create local accounts in the same way as roles-based accounts, but you check the Local User check box when creating the account.

Creating and Managing User Accounts

This section contains the following topics:

Overview for Creating an Account

Table 8-2 provides an overview of the steps you must complete to create a new roles-based administrator account.

Table 8-2   ***Checklist for Creating a Roles-based Administrator Account***

Task	Additional Information and Instructions
1. Create a new account.	Creates an account on the system with a specific username, password, and privilege level. For more information, see the "Creating a New Account" section on page 8-4.
2. Create a role for the new account.	Creates a role that specifies the services that an account can configure in your WAAS network. For more information, see the "Creating a New Role" section on page 8-10. If you are using an external authentication server, you can define matching user groups that automatically assign roles to users.

Table 8-2   Checklist for Creating a Roles-based Administrator Account (continued)

Task	Additional Information and Instructions
3. Assign the role to the new account.	Assigns the new role to the new account. For more information, see the "Assigning a Role to a User Account" section on page 8-12. If you are using an external authentication server, you can define matching user groups that automatically assign roles to users.
4. Create a domain.	Creates a domain that will specify the WAEs, device groups, or AppNav Clusters that the new account can manage. For more information, see the "Creating a New Domain" section on page 8-14.
5. Add an entity to the domain.	Adds one or more WAEs, device groups, or AppNav Clusters to the domain. For more information, see the "Adding an Entity to a Domain" section on page 8-15.
6. Assign a domain to a user account.	Assigns the domain to the new user account. For more information, see the "Assigning a Domain to a User Account" section on page 8-15. If you are using an external authentication server, you can define matching user groups that automatically assign domains to users.

Working with Accounts

When you create a user account, you enter information about the user such as the 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 WAAS Central Manager.

Each user account can then be assigned to a role. A *role* defines which WAAS Central Manager GUI configuration pages the user can access and which services the user has authority to configure or modify. The WAAS Central Manager provides one predefined role, known as the admin role. The admin role has access to all services. A *domain* defines which entities in the network that 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.

In addition to user accounts, you can create user groups if you are using external authentication of users on a TACACS+ or Windows domain server (not a RADIUS server). By creating user group names that match the user groups that you have defined on the external authentication server, WAAS can dynamically assign roles and domains to users based on their membership in a group as defined on the external authentication server. You do not need to define a role or domain for each user individually.

Two default user accounts are preconfigured in the WAAS Central Manager. 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. Only an account that has been assigned the admin role can create other admin-level accounts.

The second preconfigured user account is called *default*. Any user account that is authenticated but has not been registered in the WAAS Central Manager obtains the access rights (role) assigned to the default account. This account is configurable by an administrator, but it cannot be deleted nor its username changed. Initially, the default account has no access to GUI functionality because it has no roles defined, though it can log into the WAAS Central Manager GUI.

This section contains the following topics:

- Creating a New Account, page 8-4
- Modifying and Deleting User Accounts, page 8-6
- Changing the Password for Your Own Account, page 8-6
- Changing the Password for Another Account, page 8-7

Creating a New Account

The first step in setting up an account is to create the account by specifying a username and selecting whether a local CLI account is created at the same time. After the account is created, you can assign roles to the account that determine the WAAS services and devices that the account can manage and configure.

Table 8-3 describes the results of creating a local CLI user when setting up an account.

Table 8-3   Results of Creating a Local User

Action	Result
Creating a Local User	• The account can be used to access the WAAS CLI, WAAS Central Manager GUI (with the default role), and WAE Device Manager (if that option is selected).
	• Users can change their own passwords, and the password change will propagate to standby WAAS Central Managers.
	• The account is stored in the WAAS Central Manager database and is also propagated to the standby WAAS Central Managers.
Not Creating a Local User	• The user account is created in the primary and standby WAAS Central Manager management databases.
	• No user account is created in the CLI. Users will have to use another account to access the CLI.
	• The new account can be used to log in to the WAAS Central Manager GUI if an external authentication server is set. The user is assigned the roles defined for the default user (initially none).
	• Local users can change their passwords using the WAAS Central Manager GUI only if they have roles that allow access to the Admin > AAA section.

Note If a user account has been created from the CLI only, when you log in to the WAAS Central Manager GUI 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. An account created from the CLI initially will be unable to access any configuration pages in the WAAS Central Manager GUI. You must use an admin account to give the account created from the CLI the roles that it needs to perform configuration tasks from the WAAS Central Manager GUI.

To create a new account, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Users**.

The User Accounts window displays all the user accounts on the system.

Step 2 Click the **Create New User Accounts** icon.

The Creating New User Account window appears.

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

Step 3 In the Username field, enter the user account name.

Usernames are case sensitive and cannot contain characters other than letters, numbers, period, hyphen, and underscore.

Step 4 Complete the following steps to allow the user to access the WAE Device Manager GUI:

   a. Check the **WAE Device Manager User** check box.

   b. From the Device Manager Access drop-down list, choose one of the following options for Device Manager GUI access for this account:

   – **Read Only**—Limits this user to read only access to the Device Manager GUI.

   – **Read Write**—Allows this user to have read and write access to the Device Manager GUI.

Step 5 Complete the following steps to create a local CLI user account:

   a. Check the **Local User** check box. See Table 8-3 on page 8-4 for information about the benefits of creating a local CLI user. A local user is created on all WAE devices.

   > **Note** Do not create a local user that has a username identical to a username defined in an external authentication server that is authorizing access to the WAAS device.

   b. In the Password field, enter a password for the local user account, and reenter the same password in the Confirm Password field. Passwords are case-sensitive, must be 1 to 31 characters in length, and cannot contain the characters ' " | (apostrophe, double quote, or pipe) or any control characters.

   c. From the CLI Privilege Level drop-down list, select one of the following options for the local user account:

   – **0 (normal user)**—Limits the CLI commands this user can use to only user-level EXEC commands. This is the default value.

   – **15 (super user)**—Allows this user to use privileged EXEC-level CLI commands, similar to the functions that a Central Manager GUI user with the admin role can perform.

   > **Note** The WAAS CLI EXEC mode is used for setting, viewing, and testing system operations. It is divided into two access levels: user and privileged. A local user who has "normal" privileges can only access the user-level EXEC CLI mode. A local user who has "superuser" privileges can access the privileged EXEC mode as well as all other modes (for example, configuration mode and interface mode) to perform any administrative task. For more information about the user-level and privileged EXEC modes and CLI commands, see the *Cisco Wide Area Application Services Command Reference*.

Step 6 (Optional) In the User Information fields, enter the following information about the user in the appropriate fields: first name, last name, phone number, e-mail address, job title, and department.

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

Step 8 Click **Submit**.

A Changes Submitted message appears at the bottom of the window.

Step 9 Assign roles to this new account as described in the "Working with Roles" section on page 8-9 and assign domains as described in the "Working with Domains" section on page 8-14.

Modifying and Deleting User Accounts

✎
Note Modifying a user account from the CLI does not update the Centralized Management System (CMS) database and the change will not be reflected in the Central Manager GUI.

To modify an existing user account, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > 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. You can delete or edit user accounts as follows:

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

- To delete the user account, click the **Delete** icon in the taskbar, and then click **OK** to confirm the deletion.

  If the local user account was created using the WAAS Central Manager GUI, the corresponding user account is removed from the CLI and is also deleted from all standby WAAS Central Managers.

  ✎
  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 WAAS Central Manager GUI should always be deleted from the WAAS Central Manager GUI.

- To edit the user account, make the necessary changes to the username and account information, and click **Submit**.

Changing the Password for Your Own Account

If you are logged in to the WAAS Central Manager GUI, you can change your own account password if you meet the following requirements:

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

✎
Note We do not recommend changing the local CLI user password from the CLI. Any changes to local CLI user passwords from the CLI are not updated in the management database and are not propagated to the standby WAAS Central 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 WAAS Central Manager GUI is that both the primary and the standby WAAS Central Managers will be synchronized, and GUI users will not have to access the CLI to change their password.

To change the password for your own account, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > Security > Password**.

The Changing Password for User Account window appears.

Step 2   In the New Password field, enter the changed password. Passwords are case sensitive, must be 1 to 31 characters in length, and cannot contain the characters ' " | (apostrophe, double quote, or pipe) or any control characters.

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

Step 4   Click **Submit**.

The message "Changes Submitted" appears at the bottom of the window confirming that your password has been changed.

When you change the password of an account by using the WAAS Central Manager GUI, it changes the password for all WAE devices managed by the Central Manager.

Changing the Password for Another Account

If you log into the WAAS Central Manager GUI using an account with admin privileges, you can change the password of any other account.

Note   If you change a user password from the CLI, the password change applies only to the local device, will not be reflected in the Central Manager GUI, and is not propagated to any other devices.

To change the password for another account, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Users**.

A list of roles-based user accounts appears.

Step 2   Click the **Edit** icon next to the account that needs a new password. The Modifying User Account window appears.

Step 3   In the Password field, enter the changed password. Passwords are case-sensitive, must be 1 to 31 characters in length, and cannot contain the characters ' " | (apostrophe, double quote, or pipe) or any control characters.

Step 4   In the Confirm Password field, reenter the password for confirmation.

Step 5   Click **Submit**.

The message "Changes Submitted" appears at the bottom of the window confirming that your password has been changed.

Viewing User Accounts

To view all user accounts, choose **Admin > AAA> Users** from the WAAS Central Manager GUI. The User Accounts window displays all the user accounts in the management database. From this window, you can also create new accounts as described in the "Creating a New Account" section on page 8-4.

To view user accounts for a specific device, choose **Devices >** *device-name* and then choose *device-name* > **Device Users** or **CM Users**, depending on the device mode. The Users for device window displays all the user accounts defined for the device.

If a user account is locked out on the device, you can unlock it from this window. Check the box next to the account and click the **Unlock** button.

To view the details for an account, click the **View** icon next to the account.

Unlocking User Accounts

When a user account is locked out, the user cannot log in to the WAAS device until an administrator unlocks the account. A user account will be locked out if the user unsuccessfully tries to log in three consecutive times.

To unlock an account, follow these steps:

Step 1   From the WAAS Central Manager GUI, choose **Admin > AAA > Users**.

The User Accounts listing window appears and displays the status of each user account.

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

Step 2   Click the **Edit** icon next to the user account that you want to modify.

The Modifying User Account window appears and displays a list of devices on which this account is locked out.

Step 3   Choose the device on which you want to unlock the account.

The list of device users appears.

Step 4   Choose the user or users to unlock, and click the **unlock** button.

Working with Passwords

The WAAS system features two levels of password policy: *standard* and *strong*. By default, the standard password policy is enabled.

To change the password policy, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Devices >** *device-name* (or **Device Groups >** *device-group-name*).

Step 2   Choose **Configure > Security > AAA > Password Policy Settings**.

Step 3   Check the **Enforce stringent password** check box to enable the strong password policy.

Step 4 In the **Maximum login retries** field, enter the maximum number of login attempts to be allowed before the user is locked out. The user remains locked out until cleared by the administrator. To clear a locked-out account, see the "Unlocking User Accounts" section on page 8-8.

Step 5 Click **Submit** to save your changes.

To configure password policy from the CLI, use the **authentication strict-password-policy** global configuration command.

When the standard password policy is enabled, user passwords must meet the following requirements:

- The password must be 1 to 31 characters long.

- The password can include both uppercase and lowercase letters (A–Z and a–z) and numbers (0–9).

- The password cannot contain the characters ` " | (apostrophe, double quote, or pipe) or any control characters.

When the strong password policy is enabled, user passwords must meet the following requirements:

- The password must be 8 to 31 characters long.

- The password can include both uppercase and lowercase letters (A–Z and a–z), numbers (0–9), and special characters including ~`!@#$%^&*()_+-=[]\{};:,</>.

- The password cannot contain the characters ` " | (apostrophe, double quote, or pipe) or any control characters.

- The password cannot contain all the same characters (for example, **99999**).

- The password cannot contain consecutive characters (for example, **12345**).

- The password cannot be the same as the username.

- Each new password must be different from the previous 12 passwords. User passwords expire within 90 days.

- The password cannot contain dictionary words.

A user account will be locked out after the configured number of failed login attempts (the default is three). The user remains locked-out until cleared by the administrator. To clear a locked-out account, see the "Unlocking User Accounts" section on page 8-8.

Working with Roles

The WAAS Central Manager GUI allows you to create roles for your WAAS system administrators so that each administrator can focus on configuring and managing a specific WAAS service. For example, you can set up a role that allows an administrator to create and modify application policies but does not allow the administrator to make any other changes to the system.

You can think of a role as a set of enabled services. Make sure you have a clear idea of the services that you want the role to be responsible for because you will select these services when you create the role. Once you create the role, you can assign the role to existing accounts as described later in this chapter.

A role can give read and write or read-only access to each enabled service.

Each user account or group can be assigned to zero or more roles. Roles are not inherited or embedded. The WAAS Central Manager provides one predefined role, known as the admin role. The admin role has access to all services, similar to a CLI user that has privilege level 15. Without the admin role, a user will not be able to perform all administrative tasks.

Note Assigning the admin role to a user does not change the user privilege level to 15. The user must also have privilege level 15 in order to perform administrative tasks.

Assigning the admin role to a user grants read and write permission to all Device Manager GUI pages.

WAAS can dynamically assign a role to users based on their membership in a group as defined on an external TACACS+ or Windows domain authentication server. To take advantage of this feature, you must define user group names on the WAAS Central Manager that match the user groups defined on the external authentication server and you must assign a role to the user groups on the WAAS Central Manager. For more information on user groups, see the "Working with User Groups" section on page 8-17.

Note For user groups authenticated on a TACACS+ server to gain access to the Device Manager GUI, the user group must be configured with the admin role and the user intending to access the Device Manager GUI must first log in to the Central Manager, which creates a member account on the Central Manager and the WAE. Periodically, member accounts of a user group are removed from the Central Manager database to reduce database load, so after a period (60 days by default) of no Central Manager activity, a user will need to log in again to the Central Manager before accessing the Device Manager GUI. The cdm.remoteuser.deletionDaysLimit system property controls the removal interval.

This section contains the following topics:

- Creating a New Role, page 8-10
- Assigning a Role to a User Account, page 8-12
- Modifying and Deleting Roles, page 8-13
- Viewing Role Settings, page 8-13

Creating a New Role

To create a new role, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Roles**.

The Roles listing window appears.

Step 2 Click the **Create New Role** icon from the taskbar.

The Creating New Role window appears.

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

The name cannot contain characters other than letters, numbers, period, hyphen, underscore, and space.

Step 4 Check the check box next to the services that you want this role to manage.

The check boxes in this window are tri-state check boxes. When there is a check in the box, it means that the user will have read and write access to the listed service. Click the check box again to change the indicator to a square partially filling the check box. This indicator means that the user will have read-only access to the service. An empty square signifies no access to the service.

To expand the listing of services under a category, click the folder, and then check the check box next to the 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.

Table 8-4 lists the services that you can enable for a role.

Table 8-4   *Description of the WAAS Services*

Service	Description
Home	Allows this role to view, configure, and manage the system dashboard and settings in the Configure, Monitor, and Admin menus of the WAAS Central Manager GUI in the Home (global) context. Under each folder you can select the subpages that you want this role to manage.
Device Groups	Allows this role to view, configure, and manage the settings and subpages for the various device groups in the WAAS Central Manager GUI in the device group context.
Devices	Allows this role to view, configure, and manage the settings and subpages for various kinds of devices in the WAAS Central Manager GUI in the device context.
AppNav Clusters	Allows this role to view, configure, and manage the settings and subpages in the WAAS Central Manager GUI in the AppNav Cluster context.
Locations	Allows this role to view, configure, and manage the settings and subpages in the WAAS Central Manager GUI in the Location context.
All Devices	Allows this role to access all the devices in your WAAS network. If this service is not enabled, the user account will only have access to the devices associated with the domain that you assign to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the devices in your network. • Assigning to the account the domain that contains all the devices.
All Device Groups	Allows this role to access all the device groups in your WAAS network. If this service is not enabled, then the user account will only have access to the device groups associated with the domain that you assigned to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the device groups in your network. • Assigning to the account the domain that contains all the device groups.
All AppNav Clusters	Allows this role to access all the AppNav Clusters in your WAAS network. If this service is not enabled, the user account will only have access to the AppNav Clusters associated with the domain that you assign to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the AppNav Clusters in your network. • Assigning to the account the domain that contains all the AppNav Clusters.

Table 8-4   Description of the WAAS Services (continued)

Service	Description
Monitoring API	Allows this role to access monitoring APIs through HTTPS requests. For more information, see the *Cisco Wide Area Application Services API Reference*.
System Status	Allows this role to access the device Alarms panel. For more information about device alarms, see Chapter 17, "Monitoring and Troubleshooting Your WAAS Network."

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

Step 6   Click **Submit** to save your settings.

Assigning a Role to a User Account

After you create a role, you need to assign the role to an account (or a user group). If you create an account but do not assign a role to the account, that account can log into the WAAS Central Manager GUI but no data will be displayed and the configuration pages will not be available.

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

To assign one or more roles to a user account group, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Users** (or **Admin > AAA > User Groups**).

The User Accounts (or User Groups) window appears with all configured user accounts listed.

Step 2   Click the **Edit** icon next to the user account or group for which you want to assign roles.

The Modifying User Account (or Modifying User Group) window appears.

Step 3   Click the **Role Management** tab.

The Role Management 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 want to assign to the selected user account or group.

Step 5   Click the **Unassign** (green tick mark) next to the role name to unassign a previously assigned role.

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

Step 6   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 or group will be listed in the Roles section in the Modifying User Account (or Modifying User Group) window.

Modifying and Deleting Roles

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

To modify or delete a role, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Roles**.

The Roles window appears.

Step 2   Click the **Edit** icon next to the name of the role you want to change or delete.

The Modifying Role window appears. You can modify the role as follows:

- To delete this role, click the **Delete** icon in the taskbar.
- To edit this role, make the necessary changes to the fields, and click **Submit**.
- 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.

Viewing Role Settings

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

To view role settings, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Users** (or **Admin > AAA > User Groups**).

The User Accounts (or User Groups) window appears with all configured user accounts or groups listed.

Step 2   Click the **Edit** icon next to the user account or group that you want to view.

The Modifying User Account (or Modifying User Group) window appears.

Step 3   Click the **Role Management** tab.

The Role Management window appears.

Step 4   Click the **View** icon next to the role that you want to view.

The Viewing Role window appears, which displays the role name, comments about this role, and the services that are enabled for this role.

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

Working with Domains

A WAAS *domain* is a collection of device groups or WAEs that make up the WAAS network. A role defines which services a user can manage in the WAAS network, but a domain defines the device groups, WAEs, or file server dynamic shares that are accessible and configurable by the user.

> **Note** A WAAS domain is not the same as a DNS domain or Windows domain.

When you create a domain, you choose the type of entities that can be associated with the domain. Entity types include Devices, Device Groups, or None (for file server dynamic shares). For file server dynamic shares, the dynamic shares are assigned in the dynamic shares configuration, as described in the "Creating Dynamic Shares for the CIFS Accelerator" section on page 12-9.

WAAS can dynamically assign a domain to a user based on their membership in a group as defined on an external TACACS+ or Windows domain authentication server. To take advantage of this feature, you must define user group names on the WAAS Central Manager that match the user groups defined on the external authentication server and you must assign a domain to the user groups on the WAAS Central Manager. For more information on user groups, see the "Working with User Groups" section on page 8-17.

This section contains the following topics:

- Creating a New Domain, page 8-14
- Adding an Entity to a Domain, page 8-15
- Assigning a Domain to a User Account, page 8-15
- Modifying and Deleting Domains, page 8-16
- Viewing Domains, page 8-17

Creating a New Domain

To create a new domain, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Domains**.

The Domains listing window appears.

Step 2 Click the **Create New Domain** icon in the taskbar.

The Creating New Domain window appears.

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 Devices, Device Groups, and None. Choose **None** if this domain is used for a file server dynamic share.

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

Step 6 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.

Step 7   Assign an entity to this domain as described in the section that follows, "Adding an Entity to a Domain". If you chose None for the Entity Type, do not assign an entity to the domain, instead, the entity is used in a dynamic share configuration, as described in the "Creating Dynamic Shares for the CIFS Accelerator" section on page 12-9.

For a domain used in a dynamic share configuration, you must assign the domain to each user that needs to edit the dynamic share configuration, as described in the "Assigning a Domain to a User Account" section on page 8-15. Only users assigned to the domain will be able to edit the dynamic share.

Adding an Entity to a Domain

Once you have created a domain, you can assign an entity to the domain. An entity is either a collection of devices or a collection of device groups. You do not need to assign an entity to a domain that is used for a file server dynamic share, where the entity type is None.

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

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Domains**.

Step 2   Click the **Edit** icon next to the domain that you want to modify.

Step 3   Click the **Entity Management** tab.

The *Entity_name* Assignments for Domain window for the current domain appears.

You can filter your view of the items in the list. Filtering enables you to find items in the list that match the criteria that you set.

You can add or remove entities from the domain as follows:

- To add an entity to the current domain, click the **Assign** icon (blue cross mark) next to 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.

- 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 4   Click **Submit**.

Green check marks appear next to the entities that you assigned to the domain.

Step 5   Assign the domain to an account as described in the section that follows.

Assigning a Domain to a User Account

Assigning a domain to an account or user group specifies the entities (devices or device groups) or file server dynamic shares that the account or user group can access.

When working with a domain of type None that is used for dynamic file shares, you will need a user account for every user that needs to edit the dynamic share configuration. If you are using external authentication of users on TACACS+ or Windows domain servers, you can use user groups to more easily assign WAAS domains to users, see the "Working with User Groups" section on page 8-17.

> **Note** If the role that you assigned to an account or group has the All Devices or All Device Groups service enabled, you do not need to assign a domain to the account or group. The account or group can automatically access all the devices and/or device groups in the WAAS system. For more information, see Table 8-4 on page 8-11.

To assign a domain to a user account or group, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Users** (or **Admin > AAA > User Groups**).

The User Accounts (or User Groups) window appears with all configured user accounts or groups listed.

Step 2 Click the **Edit** icon next to the user account or group for which you want to assign domains.

The Modifying User Account (or Modifying User Group) window appears.

Step 3 Click the **Domain Management** tab.

The Domain Management 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 want to assign to the selected user account or group.

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

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

Step 5 Click **Submit**.

A green check 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 or group are listed in the Domains section in the Modifying User Account (or Modifying User Group) window.

Modifying and Deleting Domains

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

Step 1 From the WAAS Central Manager menu, choose **Admin > 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. You can modify the domain as follows:

- To delete the domain, click the **Delete** icon in the taskbar and then click **OK** to confirm the deletion.
- To modify a domain, make the necessary changes to the fields and click **Submit**.

Viewing Domains

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

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > Users** (or **Admin > AAA > User Groups**).

The User Accounts (or User Groups) window appears with all configured user accounts or groups listed.

Step 2   Click the **Edit** icon next to the user account or group for which you want to view the domain configuration.

The Modifying User Account (or Modifying User Group) window appears.

Step 3   Click the **Domain Management** tab.

The Domain Management window appears.

Step 4   Click the **View** (eyeglass) icon next to the domain name to view details about the domain.

The Viewing Domain window appears and displays the domain name, entity type, comments about this domain, and entities assigned to this domain.

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

Working with User Groups

If you are using external authentication of users on TACACS+ or Windows domain servers (not RADIUS servers), you may want to create user groups. By creating user group names that match the user groups that you have defined on the external authentication server, WAAS can dynamically assign roles and WAAS domains to users based on their membership in a group as defined on the external authentication server. You do not need to define a role or WAAS domain for each user individually; instead, you define roles and WAAS domains for the user groups, and the user is assigned the roles and WAAS domains that are defined for the groups to which they belong.

> **Note**   The dynamic assignment of roles and WAAS domains based on external user groups requires a TACACS+ server that supports shell custom attributes. For example, these are supported in Cisco ACS 4.x and 5.1 and later.

WAAS reads group membership information for each user from the external authentication server.

This section contains the following topics:

Creating a New User Group

To create a new user group, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > User Groups**.

The User Groups listing window appears.

Step 2   Click the **Create New User Groups** icon in the taskbar.

The Creating New User Group window appears.

Step 3   In the Name field, enter the name of the user group.

Ensure that the name matches the name of a user group defined on the external authentication server that you are using. Name matching is case sensitive.

> **Note**   A user group name cannot contain the following characters: # + " < > , (comma). A user group name cannot consist solely of numbers, periods (.), or spaces. Any leading periods, asterisks (*), or spaces are cropped.

Step 4   (Optional) In the Comments field, enter any comments about this user group.

Step 5   Click **Submit**.

Step 6   Assign a role or WAAS domain to this user group as described in the sections that follow.

Assigning Roles to a User Group

After you create a user group, you need to assign a role to the group. If you create a user group but do not assign a role to the group, the users in that group can log into the WAAS Central Manager GUI but no data will be displayed and the configuration pages will not be available.

To assign one or more roles to a user group, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > User Groups**.

The User Groups window appears with all configured user groups listed.

Step 2   Click the **Edit** icon next to the user group for which you want to assign roles.

The Modifying User Group window appears.

Step 3   Click the **Role Management** tab.

The Role Management for User Group 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 want to assign to the selected user group.

Step 5   Click the **Unassign** (green tick mark) next to the role name to unassign a previously assigned user group role.

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

Step 6   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 group will be listed in the Roles section in the Modifying User Group window.

Assigning Domains to a User Group

Assigning a WAAS domain to a user group specifies the entities (devices or device groups) that the users who are members of the user group can manage.

> **Note**   If the role that you assigned to a user group has the All Devices or All Device Groups service enabled, you do not need to assign a domain to the user group. The users in that group can automatically access all the devices and/or device groups in the WAAS system. For more information, see Table 8-4 on page 8-11.

To assign a domain to a user group, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA> User Groups**.

The User Groups window appears with all configured user groups listed.

Step 2   Click the **Edit** icon next to the user group for which you want to assign domains.

The Modifying User Group window appears.

Step 3   Choose the **Domain Management** tab.

The Domain Management for User Group 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 want to assign to the selected user group.

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

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

Step 5   Click **Submit**.

A green check mark appears next to the assigned domains, and a blue cross mark appears next to the unassigned domains. The domains assigned to a user group are listed in the Domains section in the Modifying User Group window.

Modifying and Deleting a User Group

To modify an existing user group, follow these steps:

Step 1   From the WAAS Central Manager menu, choose **Admin > AAA > User Groups**.

The User Groups window appears.

Step 2   Click the **Edit** icon next to the user group that you want to modify.

The Modifying User Group window appears. You can delete or edit user groups as follows:

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

- To delete the user group, click the **Delete** icon in the taskbar, and then click **OK** to confirm the deletion.
- To edit the user group, make the necessary changes to the name and comment information, and click **Submit**.
- To change the Roles assigned to the user group, click the **Role Management** tab, make the necessary changes to the roles, and click **Submit**.
- To change the Domains assigned to the user group, click the **Domain Management** tab, make the necessary changes to the domains, and click **Submit**.

Viewing User Groups

To view all user groups, choose **Admin > AAA > User Groups** from the WAAS Central Manager GUI. The User Groups window displays all the user groups in the management database. From this window, you can also create groups as described in the .